AD_____

Award Number: DAMD17-03-2-0010

TITLE: A Model Bioterrorism Civilian Medical Response: Regional
Initiatives, Readiness and Response Training and
Communications Infrastructure

PRINCIPAL INVESTIGATOR: Banu Onaral, Ph.D.

CONTRACTING ORGANIZATION: Drexel University
Philadelphia, PA 19104-2875

REPORT DATE: April 2004

TYPE OF REPORT: Final

PREPARED FOR: U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

DISTRIBUTION STATEMENT: Approved for Public Release;
Distribution Unlimited

The views, opinions and/or findings contained in this report are
those of the author(s) and should not be construed as an official
Department of the Army position, policy or decision unless so
designated by other documentation.

20040428 049

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE April 2004	3. REPORT TYPE AND DATES COVERED Final (1 Jan 2003 – 31 Mar 2004)

4. TITLE AND SUBTITLE
A Model Bioterrorism Civilian Medical Response: Regional Initiatives, Readiness and Response Training and Communications Infrastructure

5. FUNDING NUMBERS
DAMD17-03-2-0010

6. AUTHOR(S)

Banu Onaral, Ph.D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Drexel University
Philadelphia, PA 19104-2875

E-Mail: banu.onaral@drexel.edu

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Medical Research and Materiel Command
Fort Detrick, Maryland 21702-5012

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Original contains color plates: ALL DTIC reproductions will be in black and white

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 Words)

NOT PROVIDED

14. SUBJECT TERMS

NOT PROVIDED

15. NUMBER OF PAGES
206

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unlimited

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

TABLE OF CONTENTS

EXECUTIVE SUMMARY
Since its inception in 2000, the National Bioterrorism Civilian Medical Response Center (CIMERC) at Drexel University and Saint Francis University's Center of Excellence for Remote and Medically Under-Served Areas (CERMUSA) have been united in the development of rural and urban demonstration test-beds for innovative technologies related to civilian preparedness and crisis response. In this effort, CIMERC has partnered with many regional, national, government, and non-government organizations. Such strategic partnering has permitted CIMERC to extend the scope of the projects beyond just biological issues and to address the larger genre of mass-casualty incidents (MCIs). The projects presented in this report have benefited from this established and comprehensive network, as well as from the proven success of the institutions in integrating diverse interests and expertise into a large-scale initiative such as that which is inherent in biodefense. To present a coordinated front, CIMERC's efforts are driven via four concentration areas: Command and Control Operational Capabilities; Biodefense Assessment, Implementation and Evaluation; Readiness and Response Training; and Prevention and Remediation. Each of the projects presented in this report enhances the growing portfolio of projects within three of the identified concentration areas.

COMMAND AND CONTROL OPERATIONAL CAPABILITIES
Visual Imaging Enhancement for First Response
Integration and presentation of data, independent of the ambient nature, poses one of the most vital challenges in the communications arena. Work with first response teams and site commanders further underscored the incomplete and ambiguous nature of verbal communications between parties in dynamic environments intrinsic to a disaster, and thus validate the important role of imagery in disaster response. It is anticipated that **image processing** and communications will **enhance response capabilities** by providing images of the scene to appropriate liaisons in the emergency operations center and to key stakeholders. Encrypted data transmission via cellular, wireless local area network, and satellite capabilities will ensure the provision of real-time data to key stakeholders in a secure environment. CIMERC Program Objectives:
- ▲ Ongoing development of a wireless networking communications system prototype.
- ▲ Ongoing development and evaluation of a command and control system that incorporates omnicam and image-mosaicing algorithms, handheld computer programming platforms, and an image database that will establish baselines.
- ▲ Full prototype system test and evaluation.

BIODEFENSE ASSESSMENT, IMPLEMENTATION, AND EVALUATION
Rural Biodefense Response Network
Recent terrorist actions against the United States have heightened awareness against the threat of Bioterrorism among both the Armed Forces and the civilian population. The continuous threat of Bioterrorism has forced both of these populations to assess their vulnerabilities in an effort to improve their defenses and reduce the likelihood of a devastating attack. The rural civilian population has identified potential vulnerabilities that may be mitigated through the development of an improved Bioterrorism Response

Network. However, the unique needs of the nation's rural population pose many challenges to biodefense efforts. Advanced off-the-shelf interactive web-based and distance learning technologies were incorporated with work products developed from a task force effort. These products were utilized to engage key stakeholders in multivariate processes for addressing identified vulnerabilities and presenting an effective biodefense response within remote and rural areas. CIMERC Program Objectives:

- ▲ Collaborate on the establishment of the rural test bed for the development of a rural, regional civilian medical response network. Network participants will be introduced to and will assist with the development of the biological emergency preparedness self-assessment and the Biodefense Education Forum.
- ▲ Establish technology infrastructure necessary to meet communications and education requirements.
- ▲ Collaborate on the development of bioterrorism course content and delivery.
- ▲ Enhance and maintain the CIMERC website (www.cimerc.org), and incorporate appropriate security measures and SCORM-related modifications.

READINESS AND RESPONSE TRAINING
Biodefense Education Forum

When rapid evolution of information and knowledge about effective response to biological threats is compounded by the need for education and policy development across diverse communities, dynamic solutions become a necessity. In response to the need for a web-based educational system that interfaces with existing training modalities and that facilitates learning and assessment across involved communities, CIMERC proposes the creation of a **dynamic and integrated web-based learning environment**. Such an environment, by leveraging the interaction of experts with the broad user population, will permit the rapid development and dissemination of new information, policies, and assessments of preparedness concerning effective response to Bioterrorism events, along with corresponding knowledge remediation. In addition, the **Biodefense Education Forum** will provide an increased understanding of geographic challenges and cross-disciplinary issues involved in biodefense. CIMERC Program Objectives:

- ▲ Establish the framework for a repository of information concerning best practices for a local, civilian medical response to a biological challenge
- ▲ Utilize subject matter expert meetings to review and identify gaps in existing policies, protocols, and communications needs with key stakeholders.
- ▲ Further modify and integrate a policy-based self-assessment for mass casualty institutional preparedness with the Forum.

WIRELESS IMAGERY TECHNOLOGY

Introduction and Background

Biochemical agents released into the public rail system have the potential to quickly spread through several major population centers and overwhelm civilian medical communities. As such, Philadelphia's 30th Street Station is a prime target. It is centrally located within the Northeast Corridor, Amtrak's most heavily traveled rail line and carries passengers between Boston, New York City, Philadelphia, Baltimore and Washington DC. 30th Street Station is also a major hub for one of the largest secondary rail systems in the United States; the Southeastern Pennsylvania Transportation Authority (SEPTA). Each day, SEPTA connects hundreds of thousands of passengers between metropolitan Philadelphia, suburbs, rural communities, southern New Jersey and Delaware. One line of defense against bioterrorism is a *detect-to-protect* strategy where each station and train is equipped to sense the early stages of a bio-chemical attack. However, the urgency to immediately implement a system coupled with limited accuracy of existing sensors has prompted a *detect-to-treat* approach. Here, tools and protocols are developed to augment the effectiveness of emergency response communities. In line with this approach, our particular research interests for crisis management involve wireless imagery technologies to support communications between first responders and command and control (C2) nodes.

Extensive interviews with first response teams and site commanders revealed that verbal communications between parties in dynamic environments like battle spaces or disaster areas are often misinterpreted. Using a two-way radio to convey information such as situational awareness, tasking commands or resource availability can often be misunderstood or misinterpreted, because voice-based command and control creates the situational possibility that questions and answers will be vague, subjective, ill-posed, incomplete, or ambiguous. Imagery, however, can circumvent and alleviate most of these possibilities. For example, ingress and egress routes can be rapidly and unambiguously demarcated using a map highlighted with arrows and other icons. On the other hand, image-based command and control requires a communication network with multimedia transmission capability. Such a network was prototyped to acquire and process raw video data and distributes imagery (Oh, Zhang, Mode, and Jurgens, 2003). The system is based on ubiquitous and rugged wireless local area network (WLAN) and Internet technologies. The prototype can thus distribute imagery to a wide variety of devices including handheld Palm Pilots, Pocket PCs, cellular phones as well as conventional systems like fax machines.

Purpose of work

The prevailing gap in the knowledge base is that no solution provider has developed equipment that communicates visually using imagery. As such, the purpose of this effort was to enhance the prototype with the following: (1) ubiquitously acquire and distribute imagery; (2) create databases with images that establish baselines; (3) formulate guidelines for generating imagery that effectively communicates; and (4) investigate

wireless network infrastructures and protocols for real-time, reliable, and secure distribution of imagery.

Project Objectives:

The long-term objective is augmenting C2 capabilities with wireless imagery technologies. Performance of tasks like conveying situational awareness or ascertaining resources can be enhanced with today's off-the-shelf technology and equipment. One can integrate hardware like digital video cameras, microcontrollers, wireless network cards and mobile telecommunication devices and program software for computer vision, data mining and network handling. But, very few if any efforts are underway to integrate such equipment to provide a timely and useful application in command and control. The specific aims of the research were:

1. Ubiquitously acquire and distribute imagery

At any given instant, a conventional video camera only permits viewing whatever is in the direct line-of-sight. An omnicam adds a spherical mirror to capture a 180 or 360 degree field-of-view and uses image processing to un-warp a given frame. The net effect is ubiquity; omnicams can be combined with conventional cameras and permit complete visual and situational coverage.

2. Create databases with images that establish baselines

While surveillance cameras afford constant viewing of areas, the major downfall lies with the requirement that a given operator must stare at multiple monitors. For the most part scenes are uneventful and monotonous. Machine vision algorithms can augment responder's vigilance by alerting personnel when scenes change above prescribed thresholds.

3. Formulate guidelines for generating imagery that effectively communicates

Little exists industrially or academically in the quantitative definition of a useful image. A picture may be worth a thousand words but what picture must be generated to convey the correct words or relay poignant messages? Images can be useful in depicting ingress and egress routes, however too much map detail may be overwhelming while too little may yield misinterpretations. This effort will formulate tests to quantify an image's usefulness and to reveal guidelines in creating imagery that can augment communication non-verbally.

4. Investigate wireless network infrastructures and protocols for real-time, reliable, and secure distribution of imagery;

Current wireless local area network standards (802.11a,b) were developed for civilian applications. Its reliability and survivability in a disastrous environment such as the battlefield and/or a mass casualty incident needs more investigation.

Demonstration of the Need

While individual tools to acquire, process and distribute imagery are commercially available, a single system that performs all three does not exist. Such a system, customized to C2 needs, is marketable given that the architecture:

1. Delivers real-time or near real-time autonomous incident detection and its effective response during the early stages of events;
2. Performs auto detection and remote sensing for applications like biological attack and fire;
3. Disseminates information and network sensors;
4. Helps allocate resources based on the location, urgency and severity of the incident;
5. Provides information to help determine accessibility to the incident site; and
6. Provides real-time guidance and advisory.

The research and development of wireless imagery tools described in this report were particularly geared towards use in transportation system monitoring. Amtrak's 30th Street Station in Philadelphia predominantly served as the test bed for image acquisition, distribution and event monitoring.

The business case to develop such tools stem from the safety and security needs that are likely to fuel legislation for transportation systems [3]. For instance, Department of Transportation Secretary Mineta underscored the importance of intelligent vehicle technologies by pointing to the Administration's 2003 surface transportation reauthorization proposal - the Safe, Accountable, Flexible, and Efficient Transportation Equity Act of 2003 (SAFETEA). In this proposal, the Administration requests six-year funding for almost $1.7B in Intelligent Transportation Systems. Safety and security depend on persistent and pervasive monitoring. As such, wireless imagery tools that can acquire images remotely, automatically detect deviations and notify C2 transportation system authorities, have huge market potential.

Several companies including Ciber Inc., a leading international system integration consultancy, have responded to safety and security concerns. Ciber was recently awarded a $1 million contract by the U.S. Coast Guard to provide Hawaii with harbor management and security software. Similarly, Lockheed-Martin Management and Data Systems was awarded $600,000 to help plan upgrades to Pennsylvania Turnpike's operations center. In such systems, network cameras mounted around a harbor or along a highway can provide C2 with an automated means to monitor these locations. Talks with Lockheed-Martin on the application of image mosaics and pattern recognition are currently underway.

Omnicams and Mosaics

Ubiquitous acquisition can be achieved with an off-the-shelf video camera and spherical mirror. Unlike conventional cameras, which only provide a 70-degree field-of-view using wide-angle lens, the spherical mirror permits 360 degree viewing. The camera-mirror combination is called an omnicam. Much like the funny mirrors found in amusement parks, a spherical mirror results in a distorted image. Computer image processing algorithms can account for the distortion and provide unwarped views. For example, figures 1 and 2 are sample images from using a single Omnicam to ubiquitously monitor our university laboratory. A key issue is the low resolution, or the degradation in detail. Results using a variety of cameras will be presented.

Figure 1: The image reflected from a spherical mirror can be unwarped to yield a panoramic view

Figure 2: Once unwarped, particular regions-of-interest can be selected and magnified.

Mosaicing is an image processing method that essentially "stitches" different images and aligns them into a larger construct. The net effect is a single large field-of-view picture that permits more situational awareness.

Handheld Computer Program Platforms

There are currently three major handheld devices: Palm Pilots, Pocket PCs and cellular phones. The first two are equipped with MS Windows – like operating systems: Palm OS and Windows CE. Both can be easily tailored to customer needs, and offer convenient and powerful environments to program and port code across platforms. Traditionally, customers cannot program cell phones, however, Java-enabled phones are available which allow porting of Java code. Such phones are quickly becoming a mainstream mobile multimedia platform.

Java 2 Mobile Edition (J2ME) is the programming language as well as the running environment used by such cell phones. Standard Java, by definition, is a platform-independent language. The net effect is that programs written in Java can run on any device that supports the Java language irrespective of the CPU, machine and operating system. J2ME also supports mobile devices like Palm Pilots and Pocket PCs. All Java-enabled devices are compatible with J2ME, which is the key benefit of using it. Also, J2ME maintains the powerful security features found in the base Java language (J2SE) and enables wireless and small computing devices to access resources that are within an organization's firewall.

Wireless Network Test Bed

Cellular telephony systems and wireless LANs are the two major wireless networks. Cellular systems cover wide areas almost seamlessly and allow high mobility of the terminal. It primarily offers services for voice and data like Short Message Service (SMS), Multimedia Message Service (MSS) and the Internet. The data rate is still low due to the limitations of spectral resources and compactness of the phone. The wireless LAN is an extension of the wired LAN (Local Area Network). So, it has all the features of computer networks: high bandwidth, multimedia and Internet. However, the assumed terminal of the wireless LAN is a fully functional computer (primarily laptop), which has limited mobility. In addition, the wireless LAN is designed for corporative environments where "hot spots" have significant gaps.

Usually, handheld devices like the Palm Pilot and Pocket PC have wireless LAN access capability; most of them are even wireless LAN ready. The Pocket PC also has a phone edition, which means it can be a common mobile terminal roaming across the wireless LAN and cellular systems. On the other hand, the new Java-enabled phones have colorful displays and Internet access capability. If supported by service providers, it can reach a large portion of the Internet, including communications with Pocket PCs.

Full System Test and Evaluation

Pattern recognition is a technique that can automatically detect deviations from an accepted norm. In computer vision, a norm can be defined by taking many different photographs of an object. The resulting database of images characterizes the object's appearance under different lighting and weather conditions, as well as different viewing

angles. Pattern recognition is then used to compare any new photographs of the object with those in the database. Deviations above a defined threshold suggest that the object has changed. While such pattern recognition has been applied to identify faces, little work has been done to apply them to observe urban infrastructures like buildings and bridges.

There are several approaches to pattern recognition that use neural networks, statistics, multi-resolution or information theory. While each has pros and cons, the eigenface method (Turk and Pentland 1991) can be quickly applied to urban infrastructures. This method consists of weighting the difference between given and mean images obtained by averaging a predefined set of images. Pattern recognition takes place by linearly projecting the image to a low dimensional image space and weighting the difference with respect to a set of eigenvectors. If the difference (weight) is below a certain threshold, the image is recognized as known.

The full system test and evaluation for the wireless imagery technologies involved (1) acquiring images of an object with wired and wireless cameras; (2) processing these images to form the mean; (3) applying eigenface pattern recognition and (4) distributing results to wireless handhelds.

The steps involved in forming the mean involves first obtaining a set S of M images. Each image is transformed into a vector of size N and placed into the set.

$$S = \{\Gamma_1, \Gamma_2, \Gamma_3, \ldots\ldots\ldots, \Gamma_M\}$$

Once this set is obtained, the mean image ? is calculated:

$$\Psi = \frac{1}{M}\sum_{n=1}^{M}\Gamma_n$$

The difference F between the input and mean images is then computed. M orthonormal vectors best describing the distribution of the data is then calculated. A new image is transformed into its eigenface components. Input and mean images are compared and their differences are multiplied with each eigenvector. Each value would represent a weight and would be saved on a vector ?.

$$\omega_k = u_k^T(\Gamma - \Psi) \quad \Omega^T = [\omega_1, \omega_2, \ldots\ldots, \omega_M]$$

The image class that provides the best description for the input image is then determined by minimizing the Euclidean distance

$$\varepsilon_k = \|\Omega - \Omega_k\|^2$$

Pattern recognition then occurs when φ is below a threshold $?_e$. Values above the threshold dictate a deviation. In the case of applying to images of urban infrastructures, such deviations might indicate an incident or suspicious activity (i.e. an explosion, a new structure, etc.). In such cases, a deviation can be used to flag the attention of a guard or C2 personnel.

Robots:

Cameras mounted on ground and aerial robots can provide greater and more flexible fields-of-views than tripod-mounted cameras or Omnicams. An aerial robot capable of flying in and around buildings was prototyped (figures 3 and 4). The 23-gram fixed-wing vehicle flies 2 m/s and can carry a 15-gram wireless camera.
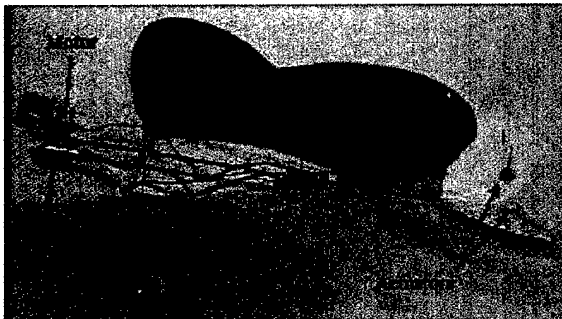
Figure 3: 23-gram fixed-wing vehicle can fly in closed quarters like warehouses, underground parking lots and airports
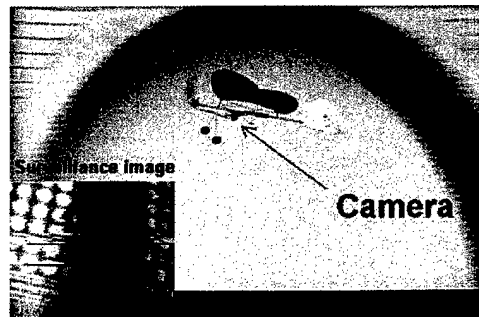
Figure 4: An on-board wireless camera can deliver photos (see inset) from an elevated position.

Flying indoors successfully demands a sensor suite to autonomously avoid collision and to localize. Towards this, sensors and control stratagems that mimic flying insects like honeybees were designed. Here, 5-gram optic flow micro-sensors (figure 5) were mounted on the aircraft. Such sensors detect the motion of texture in the field-of-view. Bang-bang control is used to navigate the vehicle in response to changes in optic flow (figure 6).
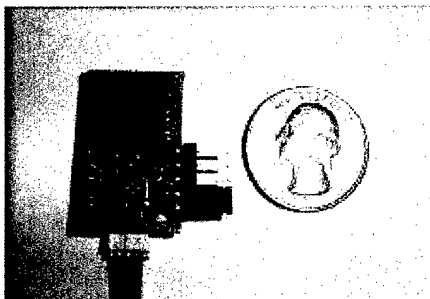
Figure 5: 5-gram optic flow micro-sensor
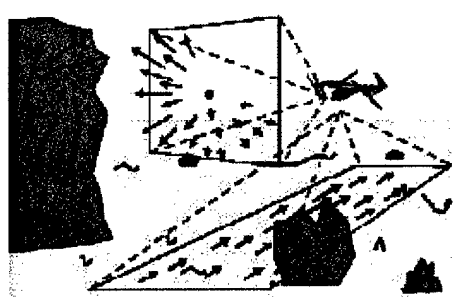
Figure 6: Sensors mounted on the nose and belly can detect oncoming obstacles and altitude

<u>Results</u>

Omnicam and image mosaicing algorithm outcomes

As stated previously, image detail is proportional to resolution. However, higher resolution images require larger transmission bandwidth. The Omnicam comes equipped with a 1.3-megapixel resolution, network ready camera called the IQeye. Both indoor and outdoor field tests were conducted to compare the resolution of IQeye with a Sony Cybershot (3.3-megapixels) and Sony MiniDV Handycam.

Figure 7: Outdoor results from attempting to view a license plate using the IQeye (left), Cybershot (middle) and MiniDV Handycam (right)

Outdoor tests were performed to view car license plates that were approximately 40 feet away from the camera (see figure 7). The IQeye has the lowest resolution of all three. The image file sizes were 24.8 KB (IQeye), 9.71 KB (Cybershot) and 8.52 KB (Handycam). An advantage of the IQeye over other network cameras is that it has a greate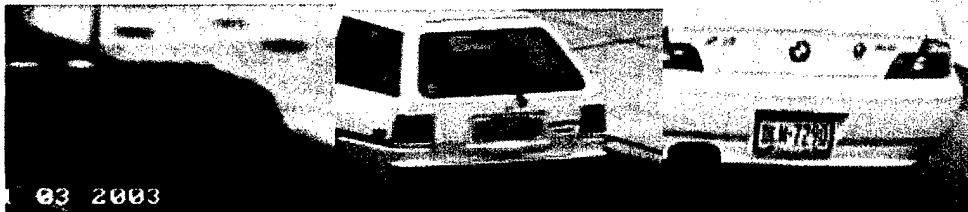r field of view, and progressive scans of moving objects are crisper than the competition. The IQeye is also capable of HDTV images with the downside that it lowers the rate that the images are transmitted (2 frames/sec). The camera can also be set for day and night modalities.

Handheld Computer Program Platforms and Wireless Network Test Bed

J2ME programs for the Java-enabled camera-ready Motorola T722i phone were developed. The programs can take pictures, send them to a designated e-mail address, and retrieve pictures from designated servers with one button click. The first function makes the phone a picture sensor. A server-end program was also developed that automatically processes photo images sent to an e-mail address. The processed photos can then be distributed to designated end-users such as first responders. With the second function, the phone can be used as a handheld multimedia terminal to access the imagery information distributed by various C2 nodes.

Figures 8 and 9 reflect the procedure by which a user may take a picture and instantly send it to an e-mail account. Figures 10 and 11 further depict the procedure of going to a given URL (http://www.opensource.org/trademarks/osi-certified/web/osi-certified-120x100.png), downloading the picture and displaying it on the screen. The MIDlet is called PngViewer.
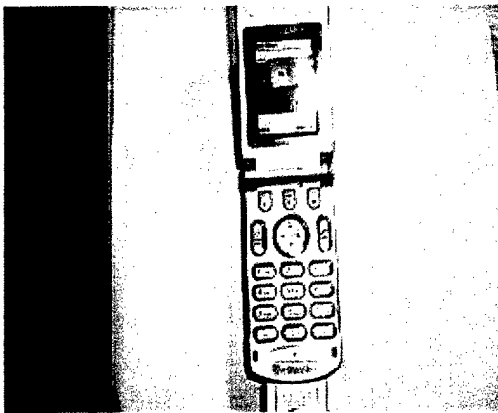
Figure 8: Picture taken by the phone
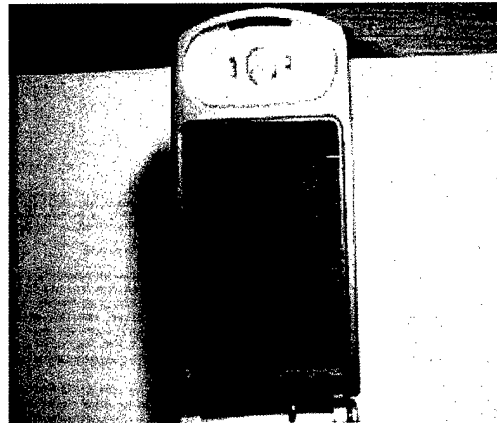
Figure 9: Sending picture to an email account
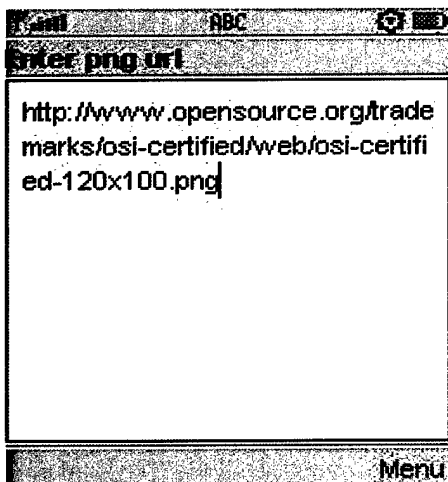
Figure 10: URL textbox

Figure 11: Retrieved & displayed image

Full System Test and Evaluation

The eigenface algorithm was applied to two cases. The first, was to images that would match closely to those in the database. This was to ensure that the algorithm was performing as designed and to ascertain threshold measures. Next, the algorithm was applied to images that were doctored with imperfections. This was performed to reflect the level of deviations that can be automatically detected.

Taking a photograph of a building every 20 minutes from 5:30 AM to 7:30 PM resulted in a set of 43 images shown in figure 12. This set was used to generate the mean image shown in figure 13. Each image was 112-by-92 pixels. The eigenface algorithm executes in 10 minutes on a Pentium 3 500 MHz PC.
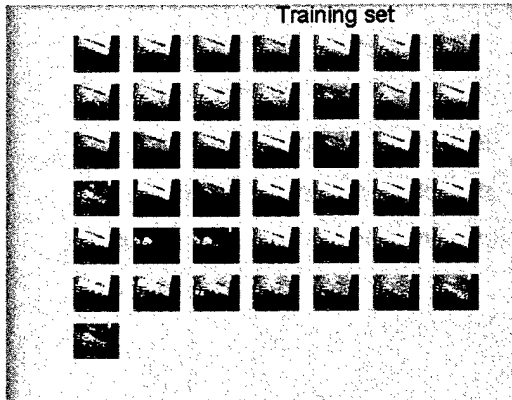
Figure 12: 43 images, acquired during one summer day, were used to form an eigenface database
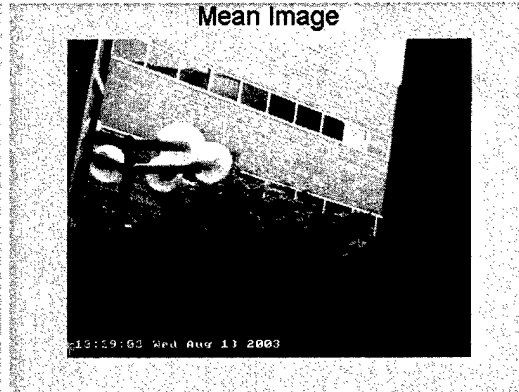
Figure 13: Resulting mean image

Figure 14 reveals pattern recognition results. The graph reveals that the error converges to zero, suggesting a match between the input image (far left) and the mean (middle).
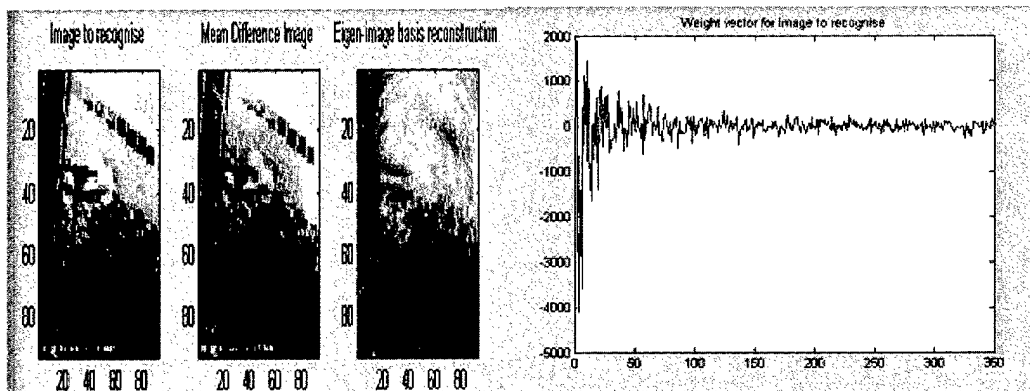
Figure 14: An input image (far left) is compared to the database mean (middle photo). Plotting eigenface results (far right) reveals that the error converges which suggests a positive match.

The weight and Euclidean distances performed on images that match reveal potential threshold values. For example, figure 15 yielded 41150 as a minimum and 42542 as the maximum Euclidean distance.
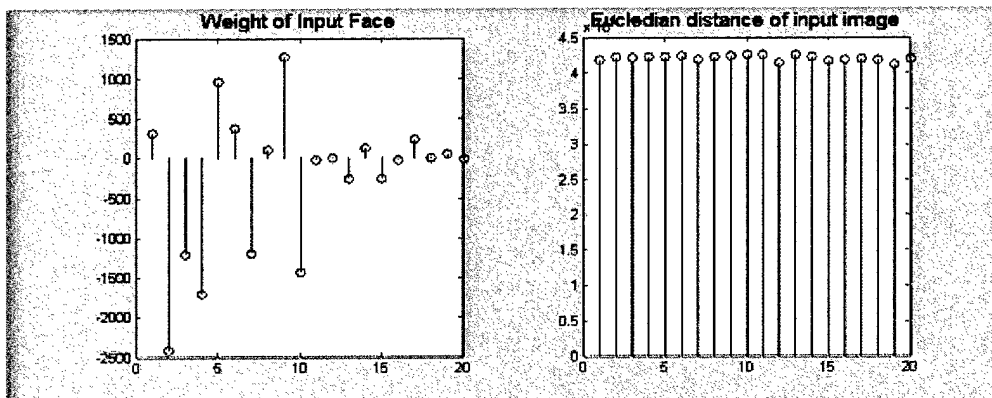
Figure 15: Results comparing an image that matches closely to images in the database. The minimum and maximum Euclidean distances are 41150 and 42542 respectively.

As such, input images that return values outside this range would suggest a deviation. For example, figure 16 reveals results using an input image that has been doctored with manually added imperfections. Such imperfections simulate the type of images that might be acquired if the building was structurally damaged.
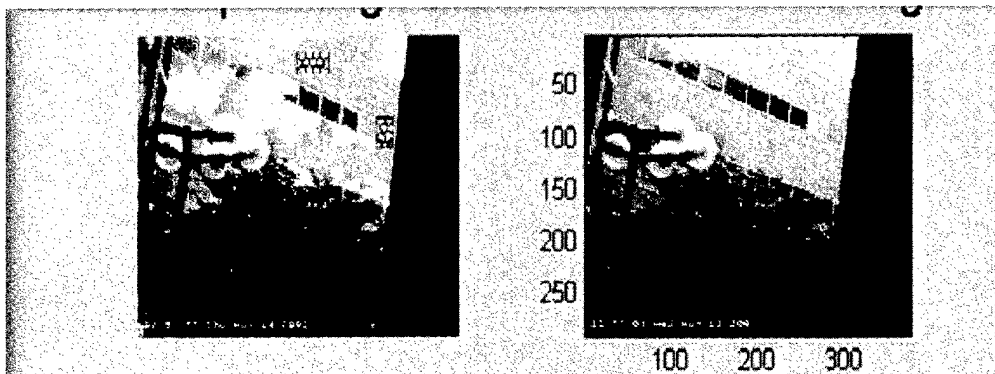
Figure 16: The input image (left) was doctored with two imperfections in the top part of the image and the image was reconstructed (right).

The eigenface algorithm detected the imperfections, yielding 42039 as a minimum and 43032 as the maximum Euclidean distance (see figure 17). Since these are outside the threshold ranges, a message would be sent to a guard to indicate a potential deviation.
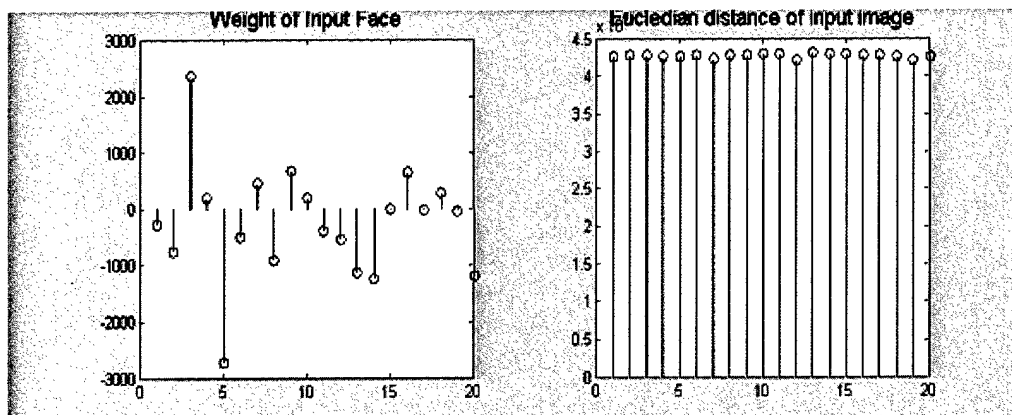
Figure 17: Results of an input image with two imperfections. The minimum (42039) and maximum (43032) Euclidean distances are above the thresholds of 41150 and 42542 respectively.

Wide ranges of images with imperfections were tested with eigenface pattern recognition. A sample of these images is given in figure 18 where minor and major imperfections were added to the windows in the building. Such doctoring simulates structural damage to the windows that could occur due to an explosion or fire. Euclidean distance calculations yielded values above thresholds and hence detected deviations.

The left image in figure 18 yielded a Euclidean distance range of (42322, 43239). The right image results in values of (43049, 44227). These values were above the norm of (41150, 42542) and hence accurately detected the presence of deviations.

Discussion

Extensive interviews with first response teams and site commanders reveal that verbal communications between parties in dynamic environments like battle spaces or disaster areas are often misinterpreted. To overcome ambiguities, a system that can acquire raw visual data, like live video and snapshots, process the data into useful visual information and distribute it to wired and wireless hardware like fax machines or handheld PCs and laptops has been prototyped. For example, pictures displaying ingress and egress routes can be wirelessly retrieved from the server and viewed remotely on handheld devices. Such pictures eliminate the need to verbally communicate, thus reducing the potential for misinterpretation.

Presently, systems that enable non-verbal communication using imagery have not been widely developed. Over the past two years, we have constructed a proof-of-concept prototype with two key capabilities; first, raw video or photos can be rapidly acquired using wired and wireless cameras and second, imagery can be quickly distributed and remotely viewed on handheld PDAs. However, the time required to transform raw visual data into distributable imagery creates a bottleneck. For example, it takes time for experts to view raw aerial photos and circle the locations of targets or threats. Such time and expertise requirements have motivated information technology research like data mining to automate the process of obtaining useful information. Open-ended problems like image understanding and decision theory form challenging gaps that prevent vertical advances in such automation. Researchers at the National Bioterrorism Civilian Medical Response Center (CIMERC) take a more pragmatic approach; CIMERC seeks to design tools that augment rather than replace personnel. Viewed in this matter, *the gap becomes a lack of tools for generating useful imagery*.

Next Steps

The long-term goal is Command and Control (C2) augmentation. Towards this goal and filling the gap, the next logical step would be to integrate off-the-shelf computer hardware, telecommunication devices and multimedia equipment to deliver C2 tools for generating imagery. The rationale stems from the fact that CIMERC researchers have a system that can acquire and distribute visual data but cannot easily and rapidly create useful imagery. Given this, *the creation of a virtual whiteboarding system* is envisioned: Color scanners can capture color pictures of whatever is written or drawn on a whiteboard; infrared receivers track and record the location of the marker's stylus on the whiteboard in real-time. A tool that enables C2 to rapidly generate useful imagery will be constructed using such off-the-shelf scanners and whiteboards.

Figure 19 is an artist conception of the virtual whiteboarding system. The circled numbers in the figure indicate the step-by-step process in transforming raw visual data into distributable imagery. (1) Raw video and snapshots of the scene captured by cameras at the scene are transmitted to C2 nodes; (2) These images are projected on a whiteboard; (3) C2 personnel write on the whiteboard, thus virtually marking up the

projected image; (4) The mark-ups are scanned into a graphic, fused with the originally projected image via image processing software, and distributed to wired and wireless
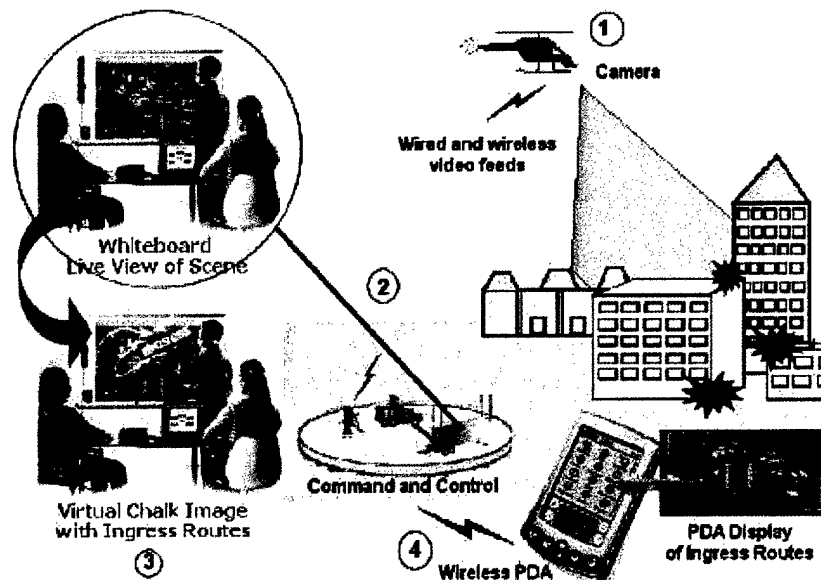
Figure 19: Artist's conception of the virtual whiteboarding system. Circled numbers depict the sequence of steps starting from acquisition of raw video to the distribution of visual information on handheld PDAs.

devices like fax machines, PocketPCs and cell phones. The result is a tool for C2 personnel to generate imagery by indirectly marking up a photo. The net effect is akin to the visuals that sports newscasters produce when commenting on plays; lines, crosses and circles mark-up the video replay to explain what the team did.

Newscasters use lightpens that activate phosphorous areas in cathode ray tube monitors. Two key limitations are first, there is no way to erase mistakes and second, lightpens cannot generate color. As such, mark-ups must be kept simple which can limit the impact and usefulness of the resulting imagery in C2 applications.

Mimeo is a commercially available whiteboard that uses an ultrasonic sensor to capture a marker's position on the whiteboard (see figure 20). A 2-foot long capture bar is an ultrasonic tracking array that mounts on the edge of the whiteboard and connects to a PC via a serial or USB interface cable. Ultrasonic transmitters embedded in the marker sleeves provide a signal for the capture bar to triangulate the pen's position on the board as the user writes. The real-time position of the pen is recorded and results in a graphic image of whatever was transcribed on the whiteboard.
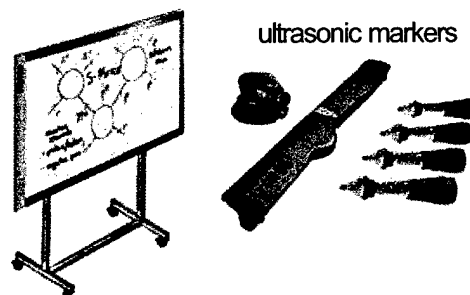
Figure 20: A graphic image depicting whiteboard content is achieved with ultrasonic position sensors

Building upon such hardware, a C2 imagery generation tool may be constructed as illustrated in figure 21. Here, the image of the given scene is projected on the white board (top). C2 then writes on top of the projected image using the ultrasonic markers. This results in a graphic image consisting of whatever was written on the whiteboard (middle). Image processing then fuses the two images which overlays the graphic image on the originally projected image (bottom). The net effect is a rapid means to generate image-based information that can then be distributed to end-users like first responders, site commanders and decision makers.

Integration Plans such as Military Applications:

The C2 prototype combined with a virtual whiteboarding system with a network of Java-enabled cell phones provides a tool to dynamically manage large-scale databases. This is especially significant to enhance battlespace diagnosis, treatment and medical management of personnel. Databases that catalog images can be created and remotely assessed thus augmenting medical awareness. A virtual whiteboard, which enables remote surgeons to highlight and mark-up pictures while viewing the operating table, would support telemedicine efforts.
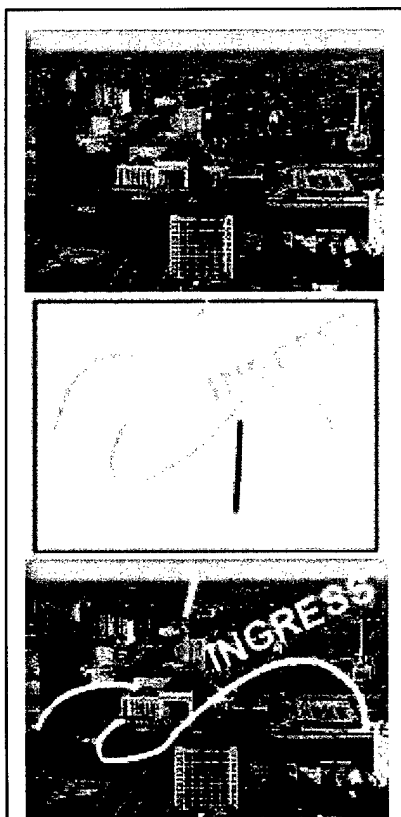
Figure 21: Original image (top) and whiteboard mark ups (middle) are fused in an image-processing step to create the imagery (bottom)

Conclusions

A prototype based on ubiquitous and rugged wireless local area network and Internet technologies was constructed and field-tested. Key components included: (1) both wired and wirelessly networked video cameras that acquire different perspectives of an environment; (2) a web server to distribute the imagery generated; (3) wireless handheld devices like Pocket PCs and Palm Pilots for downloading and viewing imagery; (4) cameras for use with omni-directional systems (5) programs that align different photos into a mosaic; (6) pattern recognition software to automatically detect events that may occur with urban structures. The net effect is an infrastructure that can acquire visual data and distribute imagery. Future work at integrating multimedia devices like virtual whiteboards will provide complementary capabilities to further facilitate C2 endeavors.

APPENDIX C1

WORKS CITED

[1] Turk, M., Pentland, A., "Eigenfaces for Recognition" *Journal of Cognitive Neuroscience,* V3, pp. 71-86, 1991.

[2] Oh, P., Zhang, R., Mode, C., Jurgens, S., "Information Technologies for Civilian Bioterrorism Response," International Conference on Computer, Communication and Control Technologies (CCCT), Volume 5, pp. 340-345, Orlando, FL, July 2003

[3] "Safety, Security concerns likely to fuel legislation for Federal highway funds" – Washington *Technology* August 26, 2002.

[4] Oh, P., Green, W.E., Yoon, S., "An Acquisition and Distribution System for Situational Awareness," *Proceedings of ASME International Mechanical Engineering Congress and Systems* (IMECE), pp. 1341-1346, Washington, DC, Nov. 2003.

[5] Green, W.E., Oh, P.Y., "An Aerial Robot Prototype for Situational Awareness in Closed Quarters," IEEE/RSJ International Conference of Intelligent Robots and Systems (IROS), pp. 61-66, Las Vegas, NV, Oct. 2003.

[6] Oh, P.Y., Green, W.E., Barrows, G., "Closed Quarter Aerial Robot Prototype to Fly In and Around Buildings," International Conference on Computer, Communication and Control Technologies (CCCT), Volume 5, pp. 302-307, Orlando, FL, July 2003

[7] Oh, P.Y., Green, W.E., "A Kite and Teleoperated Vision System for Acquiring Aerial Images," IEEE International Conference on Robotics and Automation (ICRA), Taipei, Volume 1, pp. 1404-1409, September 2003

[8] Zhou, L, Yao, Y. D., Heffes, H., Zhang. R. "Investigation of slotted Aloha under Nakagami fading with synchronized and asynchronous cochannel cells," IEEE Transactions on Vehicular Technology, Volume 52, November 2003.

[9] Petropulu, A., Zhang, R., "Blind OFDM channel estimation through Simple Linear Precoding," IEEE Transactions on Wireless Communications, 2003 (to appear).

C2 PRESENTATION

Wireless Imagery Technology Prototype

Command and Control Tools Using Wireless Imagery: An Overview
Final Report

CiMeRC

Command And Control Tools Using Wireless Imagery: An Overview

CiMeRC

Presentation Table Of Contents

Problem Statement
Approach
Methods
.
.
.
.
Conclusion

CiMeRC

Problem Statement

.
.
.

CiMeRC

Approach

.
.
.

Operational Capability

Tools to evaluate raw video from multiple wireless cameras, to automatically detect situations, and to rapidly distribute information to first responders and incident commanders.

CiMeRC

Methods
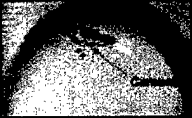
- 180° field-of-view camera
- No moving parts
- Network and wireless capabilities
- Resolution and computational limits

- Multiple images, one large view
- Hi-resolution with low-res cameras
- Automation issues

CiMeRC
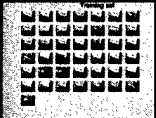
Methods

- Moving cameras provide more fields-of-view
- Flying overcomes ground obstacles
- Flying provides elevated views
- Need for autonomous navigation

CiMeRC
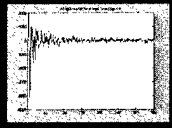
Methods

- Automatically monitor changes in a scene
- Alert personnel of suspicions deviations
- Database easily updated
- Requires sufficient archive or recursion

CiMeRC

Methods

- Portable image sensor
- Multimedia Message Services (MMS)
- JAVA enabled
- Existing universal infrastructure

CiMeRC

Methods

- T-Mobile wireless services with GPRS
- Wireless LAN
- Image server
- Cell phone and Pocket PC clients

CiMeRC

Conclusion

Omni-directional, robot-mounted and cell phone cameras can acquire images for situational awareness

Mosaicing and pattern recognition serve to automate monitoring of urban structures

Image-based information can be distributed to handheld PDAs and cell phones

Further research

CiMeRC

Wireless Imagery Technology Prototype Final Report

The project objective was to configure and assess wireless imagery technologies that would improve C2 capabilities. Towards this, specific aims were conceived and completed that: ubiquitously acquire and distribute imagery; create image databases; and investigate wireless network infrastructures and protocols for real-time, reliable, and secure distribution of imagery. The deliverables include image mosaicing systems, pattern recognition algorithms to automate urban structure monitoring, wireless network test beds and Java-enabled camera cell phones.

Click Here To View Entire Document

CiMeRC

THE NATIONAL BIOTERRORISM CIVILIAN MEDICAL RESPONSE CENTER (CIMERC) RURAL NETWORK DEVELOPMENT

Introduction and Background

The likelihood of an imminent biological or catastrophic event remains a prominent concern within today's social and political climate. Moreover, biological weapons or industrial chemical weapons continue to be considered the weapons of choice by rogue nations and dissident political groups (Cetaruk, 2003). Nationwide efforts to improve the overall readiness for such an event have focused largely on metropolitan areas. As a result, rural preparedness has changed marginally since 2001. Now more than ever, the lack of sufficient medical infrastructure, specific educational materials and individualized core healthcare training to achieve minimal competency to prepare, execute and recover from a mass casualty incident, let alone a major terrorist event, is evident.

Anticipating a need for biodefense education in the healthcare community, a rural-urban partnership was established between Drexel University and Saint Francis University in 1999. This profound dichotomy has enabled CIMERC to analyze projects in both rural and urban test beds – creating generalizable outcomes. The rural component of CIMERC is located at Saint Francis University's Center of Excellence for Remote and Medically Underserved Areas (CERMUSA), Loretto, Pennsylvania. CIMERC is a university-based consortium of medical and non-medical biodefense academics and practitioners whose emphasis is on the overall preparedness of the metropolitan and rural civilian medical community for a terrorist attack or catastrophic incident resultant in mass casualties. The rural component of CIMERC continues to support the overall preparedness and readiness of rural areas, both locally and nationwide.

The combined rural-urban experience and resources strengthens a strategic partnership in biodefense that enables continued analysis of the unique complexity of underserved rural areas. CIMERC continues to identify the inherit differences in strategies, infrastructure, preparedness, response, training and funding shortfalls within the rural areas in direct juxtaposition to their urban and major metropolitan counterparts. Furthermore, it is apparent that most of the major funding initiatives at the federal and state level are and will continue to be employed to support the present efforts in the major cities, and remains largely ineffective in reaching the local level (Hall, 2003).

Purpose of the Work

While Pennsylvania is a diverse state of rural communities, small towns and large cities, many of the areas rely on the services provided by volunteer fire, rescue and emergency service organizations, as well as part-time hospital employees. Recent studies conducted by the National Fire Protection Association (2002) estimates that nearly 73% of all emergency services are staffed entirely by volunteers and up to an additional 15% for the rural parts of the country. However, in Pennsylvania, it is estimated that 90% of the medical infrastructure for the Commonwealth operates daily

on a voluntary, non-profit and part-time basis. These national studies merely confirm what many Pennsylvanian's have known for some time: volunteer fire and emergency service and hospital practitioners provide invaluable services to countless numbers of citizens on an annual basis for little or no compensation.

As cited in the, <u>Fire and Emergency Services Task Force Report</u>, (Schweiker and Smith, 2002) "That system in which so many give so much, however faces significant challenges in the new age of terrorism." CIMERC's rural and urban task forces have identified pressing issues that necessitate leadership and solutions so that the overall health care system can prepare, execute, recover and maintain an adequate level of services during the event of a biological emergency or an attack using weapon of mass destruction.

The overall medical support system that serves Pennsylvania is a representative microcosm of the rural national problem. CIMERC is dedicated to continued improvement of the development and strategic response effectiveness of the civilian medical response community. CIMERC will continue to accomplish its mission through self-assessments, infrastructure research and development, web-based education and training, task force and forum consensus, interoperability training, communication, policy and protocol standardization and long-term technology infrastructure improvement for mass casualty incident preparedness.

Project Objectives
CIMERC strives to develop and implement a highly prepared, effective and coordinated civilian medical response to a mass casualty incident, naturally occurring event, or man-made accident through the use of standardized policy and protocol, advanced command and control, specialized education, training and a robust technology infrastructure.

CIMERC has established itself as a successful, consensus-driven outcomes-based organization through the use of local hospital/emergency medical task forces and bio-expert web forums. CIMERC has leveraged data collected from over ten years of previous and current CERMUSA prototypes and projects to enhance its development and implementation strategy in the rural community. This process has allowed CIMERC to synergize its efforts around key lessons learned, as well as the organizational experience of CERMUSA. CIMERC continues to identify the true needs of the rural medical community in an effort to solidify and streamline its organizational strategy. Ultimately, CIMERC strives to facilitate local agencies' abilities to meet or exceed benchmarks for preparedness against a bioterrorism or mass destruction mass casualty event.

Technology Empowerment

Enhancing a web-based information, education and remediation process offers the opportunity to bolster individual and organizational preparedness. CIMERC has made available via its website multiple web-based information guides, educational materials

and assessment tools to aid in the overall organizational preparedness of the rural component. As consultants in bio-preparedness, CIMERC assisted the Cambria/Somerset Task Force with a customized video and CD training package, "Are We Ready." These highly interactive, scenario-based training video and CD (Wix Pix Production, 2004) were completed to specifically address the following preparedness objectives of the rural test bed and its task force members:

- ▲ Develop a basic awareness of CBR and terrorism
- ▲ Understand the value of interaction and interoperability between field emergency medical personnel and the hospital emergency room staff
- ▲ Develop cooperation between the rural "test bed" hospitals within the Cambria / Somerset region
- ▲ Learn recommended procedures for field decontamination
- ▲ Learn procedures for site decontamination at the hospital
- ▲ Prepare for patient intake and hospital lock down procedures
- ▲ Identify a means of communication during crisis
- ▲ Understand procedures of personal decontamination and personal protective equipment

This production has the potential to reach over six counties touching over one hundred healthcare facilities, three hundred emergency medical service providers, and countless clinicians throughout greater south central Pennsylvania.

Methods

Rural Task Force, Response Network and Test Bed Participants

Two working groups and a test bed were established during this effort. The Rural Task Force, which maintains membership from local government agencies, has a primary function to plan and coordinate resources covering two rural Pennsylvania Counties. The Rural Response Network builds upon the task force membership and includes hospital and emergency response agency personnel. The primary function of the Rural Response Network is to develop and implement a multi-jurisdictional and multi-agency communications plan utilizing both technological solutions as well as traditional methods. Governor Schweiker's Fire and Emergency Services Task Force report clearly identified that infrastructure support, education and training were "key for long-term wellness and effectiveness" of the rural emergency response network. (Schweiker, 2002, CIMERC, 2003). The rural test bed encompasses a broad membership including private industry and additional university-based resources. The "test bed" is defined as the physical geographical area denoted by six counties. Participants, partners, hospitals and emergency medical service providers within the test bed, test and evaluate the products and services provided or recommended by CIMERC. The rural test bed has one essential focus: to provide continuous feedback and evaluation regarding CIMERC projects.

The relationship between the three entities known as the Rural Task Force, Network and Test Bed is unique. Personnel comprising the rural task force and response network often overlap. In other words, the membership or participants retain multiple obligations in their functional roles and responsibilities. This is not unique to rural operations; however, the percentage of persons who have multiple responsibilities is much higher when compared to urban counterparts.

The approach taken to create these entities incorporated needs for preparedness training and communications between state, region, county, and township working groups. In addition, identified personnel shortages, physical security and training were considered in the development of these working groups. All of the groups, committees or task forces are formal in nature and in some cases receive funding from external grants. Each has a chairperson and/or a co-chair who is either peer-selected, elected or a volunteer. Formal minutes are taken at each meeting and become part of the meeting record.

The Rural Task Force

CIMERC actively participates and consults in two task forces (Appendix R2): a state-level task force and a smaller county-level task force. The Federal Emergency Management Association (FEMA), Metropolitan Medical Response System (MMRS) Region 13 Weapons of Mass Destruction Working Group is the larger of the two task forces (Appendix R3a). This group is a multi-jurisdictional, multi-functional, "all-hazard" team of public health, public safety and medical professionals designed as a model for the development of other regional response teams. It is responsible for state-level policy, preparedness and training. Its membership consists of one or more persons from each county within PEMA Region 13 who meet monthly in Pittsburgh, Pennsylvania.

The second "task force" is a combination of two neighboring counties who formed one task force. The Cambria-Somerset County Task Force is a sub-group of the PEMA Region 13 Weapons of Mass Destruction Working Group with members from Cambria County and Somerset County, Pennsylvania (Appendix R3b). The task force is both a local policy and an action group. The group coordinates local training and WMD/mass casualty exercises between Emergency Medical Services (EMS) and local hospitals. It holds monthly meetings to discuss policy, materiel and educational readiness at the EMS and hospital levels. Local preparedness, resource pooling, action planning, equipment pooling, resource management, local cooperative agreements and communications, standardized equipment blocks, training, and education are all components of discussion and negotiation among the group's members. This task force identifies and prepares for the group's specific, local needs, and is represented each month at the state-level meeting in Pittsburgh by one or more task force members.

The rural task force represents the nucleus of the task forces previously discussed (figure 1). Comprised of members from the Cambria-Somerset County Disaster Management Task Force in addition to the PEMA Region 13 Weapons of Mass

Destruction Working Group, the rural task force works to increase the overall preparedness for mass casualty situations by combining local resources. The rural task force represents county level disaster preparedness expertise, as well as command and control management. CIMERC, being a nonpartisan organization, has integrated with the rural task force to coalesce local representatives into a unified group whose members are willing to share knowledge, resources, and to freely communicate information between all local health care facilities to increase the level of proficiency in response to disaster situations.

The Rural Response Network

The rural response network (Appendix R2) represents the communication and disaster management interoperability services aspect of the rural test-bed. The rural response network is a combination of county government agencies, local level departments and municipalities and senior leadership and policy makers at each of the "test bed" sites/facilities (Appendix R2). Whether at the county or at the state level, these positional leaders represent the "voices" of the rural experts. These select experts continue to actively participate in the growth and maturation of the biodefense education forum, which is the educational portal and backbone of the rural component.

The rural response network aims to execute the local preparedness plan that has been created and implemented through the efforts of the task force committee members. This critical interagency preparedness plan will use the Disaster Management Interoperability Service (DIMIS) software as its communications backbone. This service provides hospitals and emergency medical services a common communications platform delivered through a web-based solution. DIMIS, a real-time reporting service, contains invaluable data such as hospital patient census, resources committed to a disaster site, resource availability, geospatial mapping and site evaluation tools. This communications software and service was distributed to nine (9) members in the rural response network. These members were selected based on their commitment to evaluate the possibility of integrating this reporting service in the rural environment. Individuals receiving the software and service were organizational directors, such as emergency room directors, hospital safety/security officers, county-level EMS personnel, and county-level fire personnel. The DIMIS software was distributed in January 2004 and will be under evaluation until December 2004.

The Rural Test Bed

The need to gather real-time and relevant data within the rural component is paramount for long-term solution planning for rural preparedness. Providing this data and feedback of current products as well as processed and programmatic endeavors is crucial for continued support as it relates to preparedness of the rural hospitals and emergency medical services. The main role of the test bed (figure 1) is to provide continuous feedback and evaluation of the overall efforts of CIMERC as examined through the identified needs of the rural test bed. A 2002 (Joltes, K., Silveira, M) survey identified that no rural hospitals and few EMS organizations were adequately prepared for a

bioterrorism or WMD event. Based on this assessment and a call to action by Pennsylvania Governor Schweiker (2002), CIMERC provided effective tools, technology and consulting services that were otherwise unavailable within targeted rural areas. These biodefense tools were distributed within the test bed to improve the overall preparedness of rural healthcare delivery systems against any WMD or bioterrorism event (Appendix R4).

Initial equipment distribution was limited to those members who demonstrated a need for technology, were willing to participate as an active member of the test bed, and joined the rural task force. Each piece of equipment was inventoried using a unique bar code and documented in accordance with Saint Francis University's Center of Excellence for Remote and Medically Under-Served Areas's (CERMUSA) standard policy and procedure. Each recipient signed a memorandum of understanding outlining the intended use, security, data collection and reporting procedures that would accompany the issuance of the technology. Computers were delivered to each location and the local representative (Appendix R5). Sites receiving a piece of technology were designated as mass casualty staging and triage locations with decontamination capabilities.

Figure 1. An illustration of overlapping responsibilities and defining boundaries of the Rural test bed which is comprised of Cambria-Somerset County Task Force, CIMERC's rural task force, and FEMA's Region 13 Weapons of Mass Destruction Working Group.
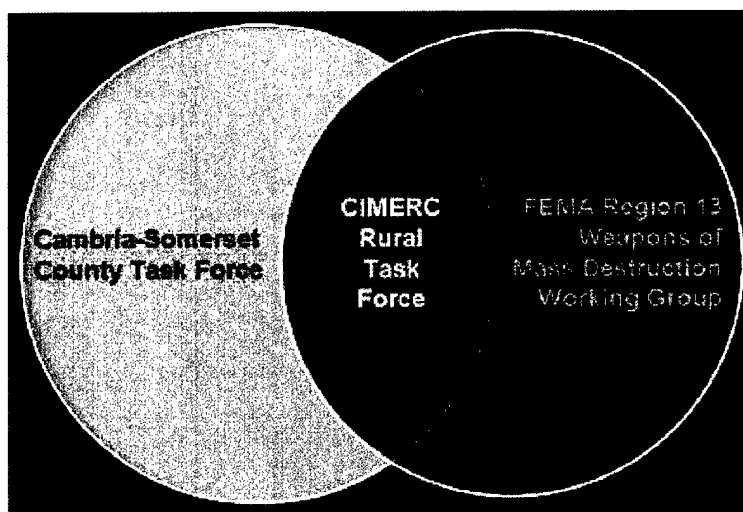
Establishment of the Rural Hospital-based Task Force and Bioterrorism Response Network

The Rural Hospital-based Task Force and Bioterrorism Response Network was established in April 2003, with the cooperation of several local rural hospitals and emergency medical service providers throughout western Pennsylvania, the Rural Task Force and Response Network began its fact-finding research. Initially, CIMERC

requested participation from each hospital located within south central Pennsylvania that actively participated in the refinement and implementation of CIMERC's "Hospital Self Assessment Tool" which can be located on the Internet at http://www.cimerc.org/content/selfAssessment.html. Due to increasing interest in this endeavor, the target audience was expanded to include neighboring medical and non-medical entities. These diverse parties commenced meeting and coordinating efforts with one common goal: to improve critical areas of communication and service delivery coordination for responding to a WMD attack, a natural or man-made biological-chemical catastrophe. Each member of the task force independently evaluated his or her own medical facilities preparedness level using the Hospital Self-Assessment Tool and reported back to the group to compare and discuss the results. This process established a baseline for work toward the previously stated common goal. Meetings were scheduled monthly on the last Thursday of each month at rotated locations depending on space availability. This schedule was maintained and modified as necessary by the sitting or acting chairperson. The structure and process of the meetings is based on a group agenda and open discussion format with minutes taken by the recording secretary to provide documentation (Appendix R4).

The evaluation results confirmed that rural healthcare facilities lacked the infrastructure and training to withstand a bioterrorism, weapons of mass destruction, man-made accident, or large, naturally occurring event (Joltes and Silveira, 2003). Based on the findings and the clear lack of basic technological infrastructure, the Task Force identified the need for the Rural Bioterrorism Response Network. The Rural Bioterrorism Response Network essentially grew out of this task force, and currently represents the communications aspect of the Rural Task Force.

The Rural Response Network (Appendix R3c) was created through the cooperation of each task force member and application of their specific skill sets. Representative from five counties in southwest Pennsylvania make up the Rural Response Network. These counties include Armstrong, Cambria, Somerset, Washington and Westmorland. Within these counties, the following hospitals are members and participants in the Rural Task Force, the Response Network and serve as principals in the rural test bed: Armstrong County Hospital, Memorial Medical Center, Miners Hospital, Windber Medical Center, Washington Hospital, Jeanette District Memorial Hospital and Latrobe Area Hospital. Together, these medical institutions serve a patient population estimated at over four hundred thousand [3.23% of Pennsylvania's populous (US Census, 2003)], while encompassing just over one-tenth of the Commonwealth's geographical area.

Technology Empowerment

Based on CIMERC's previous work, (Joltes and Silveira, 2002 and Joltes and Silveira, 2003) necessary technology infrastructure such as laptops, workstations and/or personal digital assistants (PDA's) were distributed to healthcare providers within the rural community. This initiative brought low cost technology alternatives to the rural emergency response community. Additionally, enhancing a web-based information, education, and remediation process offers the opportunity to strengthen individual and

organizational preparedness. With this initial technology intervention, rural healthcare professionals are now able to access the most current information concerning biodefense and WMD-related topics through the CIMERC website (www.cimerc.org) and the Biodefense Education Forum (http://www.cimerc.org/discuss/discussion/, username: bio-expert, password: bluespoon).

Laptop Distribution

The rural test bed/Task Force identified the following as the most important target areas for improving preparedness: improvement of technology, a source of reliable and timely information, individualized education and training programs. In response to this need, CIMERC evaluated each area of concern and formulated an action-plan to meet their needs. The identified technology need was addressed first. CIMERC provided laptop computers and personal digital assistants (PDA's) to nine of the test bed-task force sites. Through this effort, CIMERC provided the means for the given rural hospitals to access the World Wide Web, bio-specific information services, the CIMERC website and the Bio-expert's discussion forum. Furthermore, this effort enabled the hospitals to access online education, self assessment tools, and many local and federal agency resources that were inaccessible prior to this intervention.

As part of the commitment and participation of the rural test bed/task force, each member contracted with CIMERC and agreed to provide the necessary data to evaluate each medical facility's mass casualty and biological emergency preparedness and the overall impact of the intervention. CIMERC will use this critical data obtained from the rural test bed sites to evaluate its effectiveness, prior to the deployment of additional technology. CIMERC continues to leverage technology to consult with local and national entities on rural preparedness issues to help develop an effective response by the civilian medical community.

Hospital Self-Assessment Tool Integration

As part of an ongoing improvement process, a hospital self-assessment tool (http://www.cimerc.org/content/selfAssessment.html) was created through the combined efforts of Mercy Health System, Drexel University, Drexel University College of Medicine - Department of Emergency Medicine/Division of Toxicology, and Saint Francis University's Center of Excellence for Remote and Medically Under-Served Areas (CERMUSA).

Introduced early in 2003, the hospital self-assessment tool was added to the CIMERC website to provide guidance for hospital emergency departments and administrators wishing to assess their level of preparedness to evaluate and treat casualties resulting from a biological mass-care emergency. This goal was accomplished through the use of an interactive self-assessment questionnaire developed and validated by an expert consensus panel. The panel was composed of experts in the fields of emergency medicine, medical toxicology, pre-hospital emergency care, hospital administration, and counter-terrorism. The expert panel met in Philadelphia, Pennsylvania, in June of

2002. Recommendations and guidance points developed by this panel represent to date the only current, validated preparedness recommendations for hospital-based emergency departments. Responses to the self-assessment questions were derived from the Domestic Preparedness Defense Against Weapons of Mass Destruction: Hospital Provider Course manual, used by the Soldier Biological and Chemical Command's (SBCCOM) Domestic Preparedness Program.

The initial paradigm identified by the Consensus Panel is the supposition that a given hospital emergency department will be in full compliance with all Joint Commission on Accreditation of Healthcare Organizations (JCAHO) regulations addressing disaster preparedness/management, as well as any regulations addressing weapons of mass destruction. The self-assessment, derived from previously published guidelines and recommendations of the consensus conference, embodies the requirements necessary for the capability of an emergency department to generate a minimal level of reasonable response to an event.

Rural and Urban CIMERC Interface and Integration

Concerns regarding the concept and implementation of a "one size fits all" strategy were quickly dispelled by means of data collection, workshops, and conferences. In the process of developing the ideal response, realizing and understanding the uniqueness of CIMERC's rural-urban partnership became mission critical. CIMERC recognized that emergency response, healthcare delivery, technology infrastructure, educational resources, and available funding in metropolitan areas vary significantly from the rural communities. With this knowledge, technology was identified as key for interfacing and integrating assets and information between the rural and urban components. CIMERC's strategic plan continues to support initial face-to-face networking in both the rural and urban test beds with the intention of electronically relocating a core group to the Biodefense Education Forum.

In response to the need for a web-based educational system that interfaces with existing training modalities and that facilitates learning and assessment across involved communities, CIMERC is developing the *Biodefense Education Forum* (Forum). The Forum is a dynamic and integrated web-based learning environment that permits the development and implementation of highly specific education and training programs for a widely diverse group with a differing knowledge base by leveraging the interactions of experts within the broad user population. The Forum corrects weaknesses through a training remediation process and provides an increased understanding of geographic challenges and cross-disciplinary issues involved in bioterrorism response. This new cyber conference center and meeting place advances the true interface and interaction of the test beds.

CIMERC has recorded group-level data (Appendix R7) regarding the use of the website since it was first published on the Internet (15 January 2003). This data reveals that, on average:

> ▲ 110 unique www.cimerc.com users visit the site daily and visit 2.72 pages,

▲ 61 files are downloaded from this educational portal every day
▲ 95% of website visitors do so on weekdays (5% visit on weekends)

Additional data was collected about the visitor web browser use and operating system use. This information will motivate future developmental decisions about the website as its user population grows.

Course Content Development

Development and delivery of educational courses was identified by the rural task force as the next most critical, missing piece in the overall preparedness of the rural medical community. CIMERC used data collected by the task force to formulate a multi-faceted education component on CIMERC's website. A collection of five emergency response and preparedness courses now reside on the CIMERC website for public access (Appendix R6). These educational tools were used to augment existing training programs as well as offer more advanced educational courses that were not previously available. These self-study courses were developed by federal government agencies intended for a range of audiences (e.g., individual citizen, military personnel, and civilian first responder).

With the knowledge institutions gain from using the Hospital Self Assessment Tool, each medical facility is provided the data necessary to target and remediate existing knowledge gaps. Currently, several courses to help remediate knowledge gaps are offered through the CIMERC website. Additional courses are under development by CIMERC to continue meeting the ever-changing and specialized needs of the rural emergency medical and hospital response system.

Military Relevance

The United States Armed Forces and Department of Defense (DOD) often operate in geographically isolated and underserved areas. The location of the remote areas often hinders the rapid transmission of education, training, and information that is vital during a time of critical decision making or during conflict. The development of a rural model may provide the DOD with several alternate paradigms for cost-effective central training, centralized information structure, education, and integration of information technologies in remotely located, underserved or forward deployed military installations throughout the world.

Discussion

With this initial technology intervention, rural healthcare professionals are now able to access the most up-to-date information concerning bioterrorism and WMD-related topics through the CIMERC website and CIMERC's Biodefense Education Forum.

However, additional resources are necessary for the orchestration of a real-time response within the rural network. Each health care facility has identified and prioritized its own needs, as related to mass casualty preparedness. Additionally, the organizations that represent pre-hospital providers have followed the example of the local hospitals and have completed their own prioritized list of needs. The summary of data gathered during two regional expert discussion meetings (Appendix R4) continues to support the need for a significant increase of individual and institutional preparedness. The top issues that both hospital and pre-hospital providers agreed upon were:

- Increase funding from state and federal agencies.
- Technology and Internet access (computers, PDA's, software).
- Standardized education pipeline (basic to advanced).
- Peer-to-peer information and resource sharing (live and virtual).
- One-stop shopping website that provides above needs.

Enhance System and Content Security

The CIMERC web service offering has improved significantly throughout the 2003 calendar year; the system was upgraded from a basic flat HTML-based proof-of-concept residing on a Windows-based server to a more highly-structured, interactive environment using production grade Linux systems. This upgrade is in accordance with plans established in the last months of 2002, and reflects a growing awareness of the need for a stable, secure production environment. Further development of the security infrastructure is needed due to the evolution of the software and methodology. The *CIMERC Production: Web Services Design* (April 2003) and its addendum (December 2003) offers additional detail regarding pre-production planning and the basic tenets used to develop the system in its current form (Appendix R8).

Enhance Technical Functions

New hardware was purchased in June 2003 to enhance the CIMERC web service. The hardware consisted of paired HP server-class systems with redundant power supplies, RAID arrays, and other features that will permit a higher level of availability than a standard desktop PC. Two servers were designated specifically for the web service (Apache), while two others house the back-end Sybase database engine that provides a repository for the Biodefense Education Forum. The paired systems are matched from a hardware standpoint to achieve commonality of components and ease of management.

As planned, Red Hat Linux was installed on these systems since its security features are considerably greater than those available under the Windows family of products. Version 9 was installed, along with all patches and utility updates available when the installation was performed. A regular schedule was established to ensure that software

patches, especially those salient to the security component of the system, are first tested on a non-production server and then applied on a consistent basis.

Each production system is connected to an uninterruptible power supply (UPS) system to provide clean power and to protect against short-duration power outages or brownout conditions. The operating system monitors UPS and power status and will be established to power down the systems automatically if conditions arise that require this action. However, the CERMUSA facility has its own back-up generator system; this feature should never be needed.

The Saint Francis campus now has multiple connections to the Internet (one via the new Internet-2 infrastructure) and the other (via a dedicated T-1) to provide redundant access to the backbone of the nations information super highway. Each connection is provided by a different internet service provider (ISP) or carrier. This configuration virtually eliminates the possibility of a single point of failure and dramatically increases reliability and access to the CIMERC website (Joltes, 2003).

<div align="center">Conclusions</div>

A sound response to any event that threatens human life and health, in particular to a mass casualty incident (MCI), requires a well-trained and resourceful workforce. CIMERC proposes education and policy-based efforts in the Readiness and Response Training concentration area to bolster MCI readiness and response preparedness. CIMERC continues to recognize the vast differences and unique needs of the nation's rural population.

Examining the results of over ten years of research at CERMUSA, it is clear that continued infrastructure support should be provided in an effort to bridge the technology gap within the rural emergency response community. A continued technological infrastructure paradigm shift in rural localities is needed to enable new strategies for delivery of real time informatics, to provide just-in-time education and training, to increase overall awareness, to better prepare communities for response to major emergencies like infectious disease outbreaks (intentional or naturally occurring), and to enhance local communication in the rural environment.

The rural technology infrastructure, often characterized by stand-alone systems and dial-up Internet connectivity, is in critical need of enhancement. However, a strategic technology needs assessment is warranted to determine the best methods to resolve technological disadvantages. To understand the effect of technology distribution completed during this effort, a follow-up evaluation will be combined with the strategic needs assessment for the best use of future resources. In addition, additional upgrades to emergency response planning tools are necessary for continual improvement.

Based on results of this effort and feedback from focus group participants, enhanced development of the Biodefense Education Forum is recommended. Forum software

and program code will be enhanced to accommodate additional users and new features to the portal. Additionally, experts will be recruited, trained, and maintained to expand the working knowledge and human component of the Forum. It is this feature that will encourage community development and set the Forum apart from other interactive community-driven websites.

APPENDIX R1

WORKS CITED

Fire protection in rural America: A challenge of the future, National Association of State Foresters. (2001). Medford, MA.

Cetaruk, E., (2003). Toxic gases in your community, Chemical Agents of Opportunity for Terrorism: The medical and psychological consequences of TICs (Toxic Industrial Chemicals) and TIMs (Toxic Industrial Materials). American College of Medical Toxicology, Fairfax, VA.

Chairperson, (2003). Rural PA Region 13 Metropolitan Medical Response System Working Group meeting minutes, Pittsburg, PA

National Bioterrorism Civilian Medial Response Center, (2003). Enhancement the civilian medical communities response during the earliest of a bioterrorism attack (DOD Report No. 233-01-00065). Philadelphia, PA

Hall, M. (2003). Homeland Security Money Doesn't Match Terror Threat, USA Today, Zanesville, OH.

Joltes, K., Silveira, M., (2002). Rural Hospital Bio-Terrorism Preparedness Survey Instrument, Saint Francis University, Loretto, PA.

Joltes, K., Silveira, M., (2003). Hospital self assessment tool results. CIMERC

Joltes, K., Silveira, M., (2003). Rural Biological Preparedness Survey Update. CIMERC

Joltes, K., Silveira, M., (2003). Rural Taskforce / Response Network Memorandum, Saint Francis University, Loretto, PA

Joltes, R. (2003). CIMERC Production Web Services Status Report and Future Planning, Pittsburgh PA

Jurgens, S. M., Schaben, C. P., Silveira, M., (2003), Bio-Experts Discussion Forum Conference (Rural), CIMERC, Saint Francis University, Loretto, PA.

Jurgens, S. M., Schaben, C. P., Silveira, M., (2003). Bio-Experts Discussion Forum Conference (Urban), CIMERC, Drexel University Philadelphia, PA.

Martin, T., (2003). Food and water as vehicles for chemical terrorism? Chemical Agents of Opportunity for Terrorism: The medical and psychological consequences of

TICs (Toxic Industrial Chemicals) and TIMs (Toxic Industrial Materials). American College of Medical Toxicology, Fairfax, VA.

Nelson, L., (2003). Clinical Neurotoxicology of Chemical Weapons, New York City Poison Control Center, NY, NY.

Onieal, (2000). US Fire Department Profile, National Fire Protection Agency, Quincy MA.

Sako, (2002). Pennsylvania Emergency Management Agency (PEMA) Study of Volunteer Fire and EMS for Pennsylvania, Harrisburg, PA.

Smith, D., (2002). Pennsylvania Senate Committee on Communications and Higher Technology, Harrisburg, PA.

Smith, Schweiker, (2002). Fire and Emergency Services Task Force, Harrisburg PA.

Smith, Schwieker, (2000). Fire Protection in Rural America, National Association of State Foresters, Medford, MA.

United States Census Bureau. (December 2003). Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2003. [Online], Population Division.
Available: http://eire.census.gov/popest/data/states/tables/NST-EST2003-01.php

Wax, P., (2003). Toxic warfare: Looking beyond conventional chemical weapons. Chemical Agents of Opportunity for Terrorism: The medical and psychological consequences of TICs (Toxic Industrial Chemicals) and TIMs (Toxic Industrial Materials). American College of Medical Toxicology, Fairfax, VA.

Chemical Agents of Opportunity for Terrorism, The Medical and Psychological Consequences of Toxic Industrial TICs and Toxic Industrial Materials TIMs Oct 28, 2003. Funded through the ATSDR division of the Health Education and Promotions National Organizations cooperative Agreement Program in collaboration with the ATSDR office of the Assistant Administrator Terrorism Response Activity. Paul M. Wax Course Director.

APPENDIX R2
RURAL PERSONNEL INFRASTRUCTURE

The Rural Task Force:

▲ The Pennsylvania Emergency Management Agency Region 13 Weapons of Mass Destruction Working Group

▲ The Cambria-Somerset County Disaster Management Task Force

The Rural Response Network:

▲ Cambria County 911 Center
▲ Somerset County 911 Center
▲ HAZMAT Response Team
▲ SHARP Response Team
▲ Cambria Department of Emergency Services
▲ Somerset Department of Emergency Services
▲ Conemaugh Health Systems
▲ UPMC Lee Hospital
▲ Johnstown Fire Department
▲ Cambria Transit Authority
▲ Southern Alleghenies Emergency Medical Services
▲ 7th Ward EMS
▲ West End EMS

The Rural Test Bed:

▲ Saint Francis University's Center Of Excellence For Remote and Medically Under-Served Areas
▲ Cambria County 911, Assistant Director
▲ Cambria SHARP/HAZMAT Team, Director
▲ Memorial Medical Center, Director of Trauma Services Memorial Medical Center
▲ Miners Medical Center, Director of Emergency Services, Miners Hospital
▲ Windber Medical Center, Director of Safety Windber Medical Center
▲ Latrobe Area Hospitals, Medical Director, Latrobe Area Hospital
▲ Meyersdale Medical Center, President, Meyersdale Medical Center
▲ Armstrong County Memorial Hospital, Director of Emergency Services,
▲ Jeannette District Memorial Hospital, Pre-hospital Services Jeannette District Memorial Hospital
▲ Loretto Emergency Medical Services, Director
▲ University of Pittsburgh Public Health Center, Assistant Director
▲ Chem Image Co, Associate Director
▲ InSORS, Technology Group, President for Government Services

APPENDIX R3

MAPS OF REGIONAL WORKING GROUP AND TASK FORCE SERVICE AREAS
IN RURAL PENNSYLVANIA

MAP OF FEDERAL EMERGENCY MANAGEMENT AGENCY (FEMA)
METROPOLITAN MEDICAL RESPONSE SYSTEM (MMRS), REGION 13

Federal Emergency Management Agency (FEMA), Metropolitan Medical Response System (MMRS) Region 13 (bold border): A Geographic Comparison with Pennsylvania Emergency Management Agency (PEMA) Counter Terrorism Task Forces
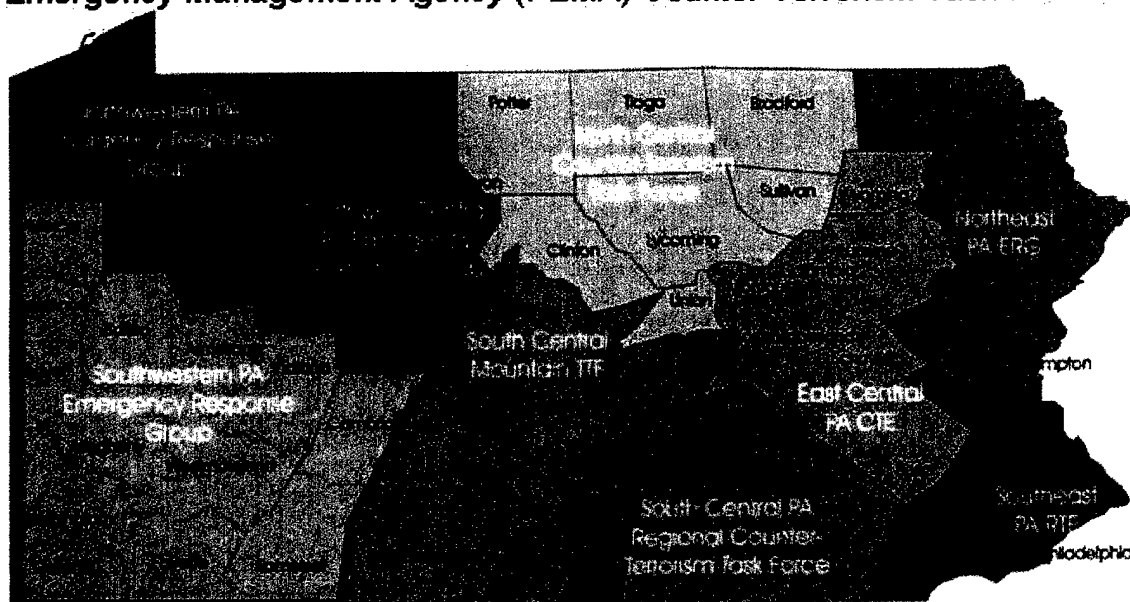
MAP OF CAMBRIA-SOMERSET COUNTY TASK FORCE SERVICE AREA

Cambria-Somerset County Emergency Management Task Force (dashed border):
A Geographic Comparison with the Federal Emergency Management Agency (FEMA), Metropolitan Medical Response System (MMRS) Region 13
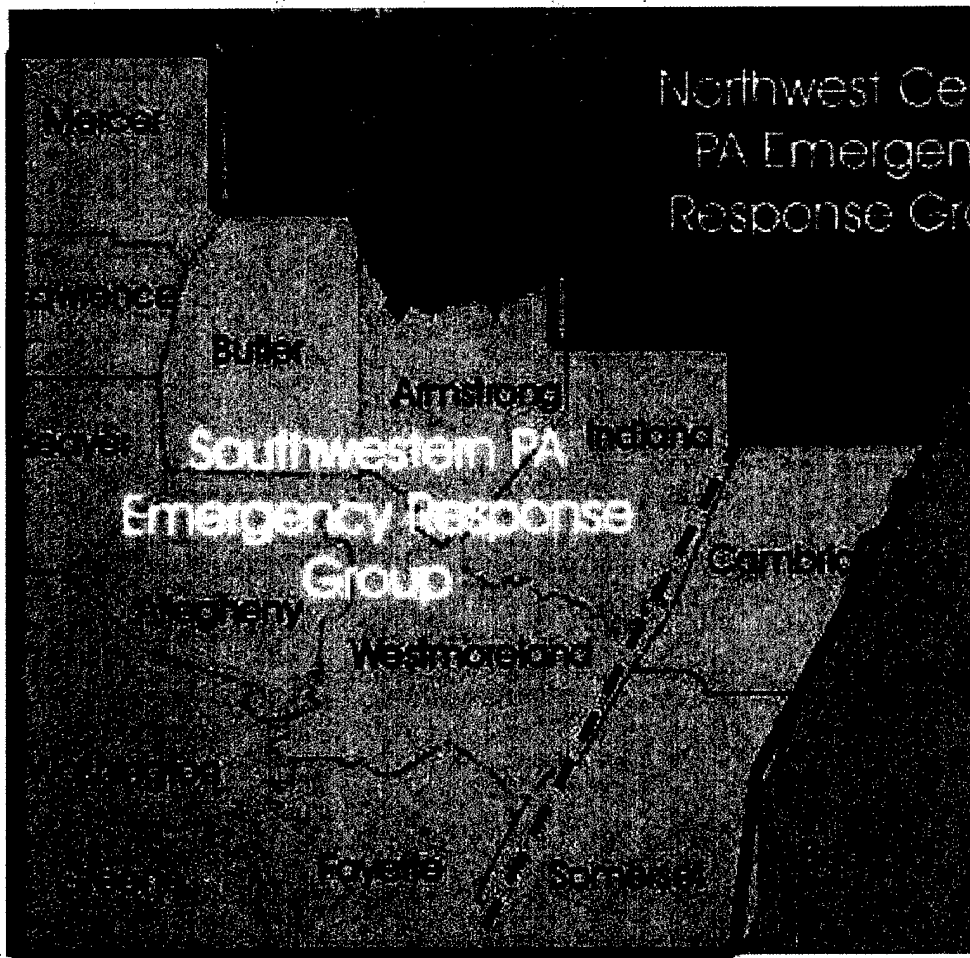
APPENDIX R3c

MAP OF THE RURAL RESPONSE NETWORK SERVICE AREA

Western Pennsylvania Counties Represented in the Rural Response Network
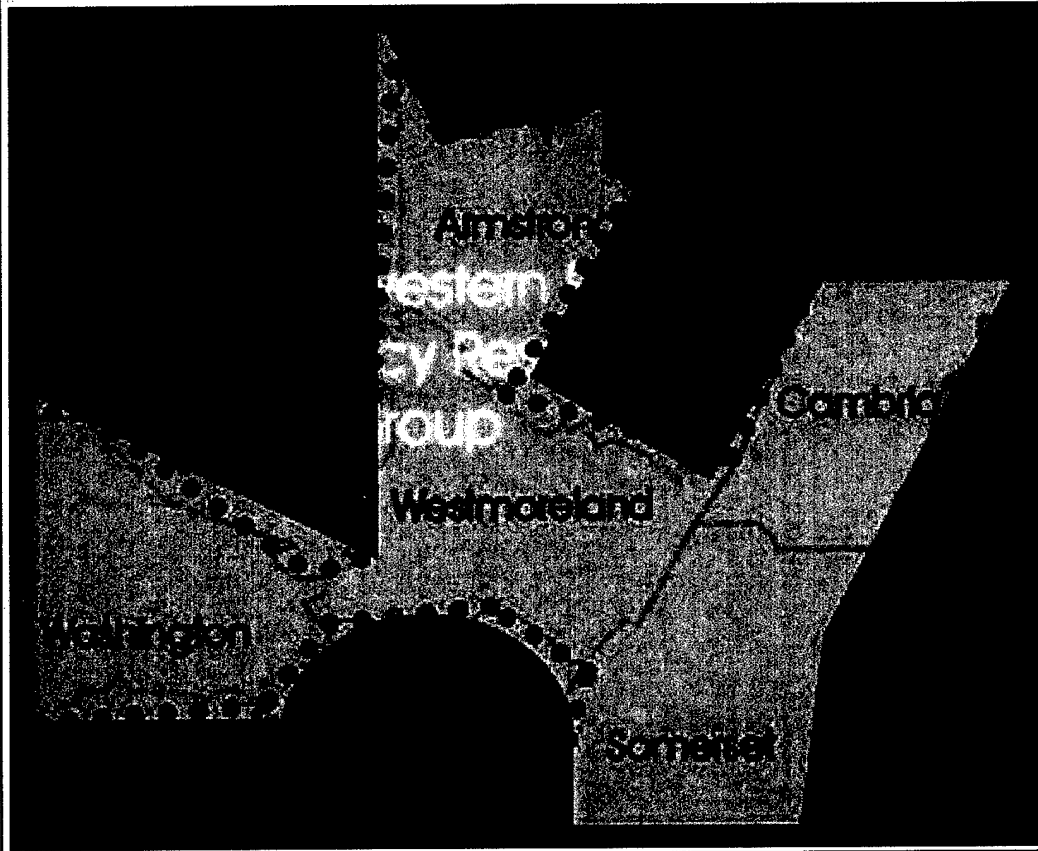
APPENDIX R4

CAMBRIA SOMERSET
DISASTER MANAGEMENT TASKFORCE

January 29, 2004

The meeting was called to order at 0900 by Patti DeFrehn.

Members in attendance: P. DeFrehn, S. Nagle, S. Benza, L. White, R. Springer, M.Huss, B. Feist, R. Shinholt, S. James.

HRSA Funding: Budgets and worksheets had to be completed this month with retrospective actions to August 2003. Most of the hospitals present stated monies are to be used for further decontamination, communication and security. Unknown when monies will become available.

Non-Allegheny Co. Hospital meeting: Held at Hospital Council on January 9, 2004. Extremely beneficial to talk with other facilities discussing same concerns. Our current county taskforce model was applauded and recommended by V. Tucci to be used region wide. It was discussed by all participants that communications between Region 13 meetings to the MMRS is extremely important. A discussion also occurred that county EMA officials should be communicating with hospitals within their county on issues.

MMRS Meeting Update: Held on January 15, 2004 at Allegheny County EOC. Committees have been formed and it is the recommendation of this group that we have a representative on each committee. The committees are as follows:

-Hospital: Integration of community hospital best practices and coordination of purchasing to meet needs.

-Prehospital: Patient ID and tracking/Triage tags

-Special Needs, Mental Health, and Children

-Strategic National Stockpile

-Technology Integration: interoperable communications and healthcare reporting

-Equipment: standarization of purchasing of equipment

-Education and Training

-Military/Civilan Relations

-Grants and other funding sources

EMA Update:

Johnstown City: Chief Huss stated funding has been put into place for the city to purchase two Zumro tents

Cambria County: R. Springer discussed a meeting at the airport this past week in which a decision was made to have two drills this spring. The first will be a tabletop exercise with a full scale exercise to follow. There will be an upcoming meeting in February where hospital representatives will be invited.

Somerset County: R. Shinholt suggested and the group agreed that we need participation in this taskforce by all six hospitals and both EMA's. A letter will be sent to the hospitals not in attendance of the need for commitment to this taskforce.

County Commissioner Invitation

Discussion occurred regarding inviting a representative of each county commissioners office to the next meeting. A letter of invitation will be sent with copies to M. Huss and R. Lohr.

HAM Radio Update

S. Nagle discussed a recent meeting she had with Barry Rummel who is the HAM operations representative for Cambria County. He is very willing to assist with purchasing and set up of these radios for the hospitals to enhance communications during an event. It was the recommendation of this group to continue discussions and pricing the radios.

PPE Update

Conemaugh Memorial Medical Center will be having PPE refresher courses in the month of February. The dates and times are as follows:

February 10   0800-0900   1400-1500
February 17   0800-0900   1400-1500
February 24   0800-0900   1500-1600

All classes will be held in the ER conference room and anyone is welcome to attend.

Training for EMS PPE

B. Feist discussed the training in conjunction with Bucks County Community College will occur at various sites in February, March, and April for EMS providers to obtain their PPE that is

allotted by Region 13. A letter will follow. Currently R. Shinholt from Somerset Co. said there is no plans for training of EMS in Somerset county and he is not sure when the PPE will be given out.

Update on Interactive CD

T. Doyle and C. McIlhenny from WixPix presented the completed version of the interactive CD. Much hardwork and time have been placed into this production to make it a quality educational tool. Within the next several weeks, hospitals and EMS will be obtaining copies of the CD which CERMUSA has graciously donated monies for.

Equipment Review

C. Hayduk from Fisher Safety brought several new pieces of equipment including a roller table for decontamination of non ambulatory patients and a communication device for personnel in PPE. He is willing to attend any educational sessions hospitals in our area may be having and will answer any questions.

The meeting adjourned at 1110 with no further business. The next meeting will be scheduled for mid March with an exact date to follow.

Respectfully Submitted.

Storm Nagle

CAMBRIA – SOMERSET DISASTER MANAGEMENT TASKFORCE MEETING

The Cambria – Somerset Disaster Management Taskforce Meeting was held on December 11, 2003 at 0900 in the MMC Department of Emergency Medicine Conference Room.

Present: V. Wiltrout, R. Shinholt, D. Fox, L. Stinson, S. Benza, J. Mackalus, S. Nagle, A. Kovacic, S. James, R. Springer, C. Moen, P. DeFrehn

		ACTION/FOLLOW-UP
HRSA Funding Update / Reminder	Patti reminded everyone that the HRSA Grant Budget form must be completed by the end of the year. Vicky has contacted Chris Hayduk at Fisher Safety requesting information on any new bioterrorism equipment. Ideas from Chris and others at the meeting include: ▪ Automatic lockdown equipment ▪ Cartridges for Level B Suits ▪ Drill Costs and Training exercises ▪ Decon Carts for unconscious patients ▪ Hazmat Smart Strips ▪ Communications Devices to be used with Level B Suits ▪ Outside Lighting ▪ Stronger Collection Pools ▪ Outside Clocks ▪ Possibly Group effort for education ▪ Communication Equipment	
Update on Interactive CD	Patti informed the group that the CD will be completed in late Dec or early Jan. Additional costs were paid by CIMERC. Mark Silveira from CIMERC has asked to join the committee.	The committee unanimously agreed that it would be an asset to have Mark Silveira join the committee.
November 12 Drill Overview	Storm felt it was a very educational exercise for the hospitals that actually got patients. She also felt that drills should be done quarterly to keep everyone current. One problem identified at MMC was that the tent inflation tube broke, and Storm suggested a spare tube might be a good idea. Storm also suggested that the use of ancillary personnel instead of all nurses in decon. It is not necessary for nurses to do decon if ancillary personnel are available, and for unconscious patient it would be beneficiary to have more men (assuming most of our nursing staff are women). Judy and Ron were both present at Minors and stated that the hospital employees, as well as the fire department, learned a lot as a result of the drill.	The drill sub-committee will continue to meet and discuss the possibility of quarterly drills.
Hospital Meeting at HCWP	Patti suggested that each hospital should have a representative at this meeting and several members are planning to go.	
EMA Update	Ron Springer informed the group that they will soon be inservicing the 700 Cambria police officers. After training each	

	police officer will receive a PPE kit with a level B suit. Rick Shinholt reported that Somerset county has received parts of suits but has not yet received any complete suits and has not scheduled any inservicing.	
Communications	The use of amateur radios for communication between the hospitals during an event was discussed. It was decided that during an event this may be the only way to communicate.	Ron Springer suggested that when completing the funding form each hospital designate between $1,000.00 - $2,000.00 for hand radio equipment.
Next Meeting	The next meeting will be held at the end of January, date and time to be determined.	

Respectfully Submitted By: Vicky Wiltrout.

THE NATIONAL BIOTERRORISM CIVILIAN MEDICAL RESPONSE CENTER
(CIMERC) RURAL BIO-EXPERTS FORUM MEETING
07 NOVEMBER 2003
At
**Saint Francis University's Center of Excellence For Remote and Medically Under-
Served Areas (CERMUSA), Loretto Pennsylvania**

Objective:

*Solicit input from the rural medical community in order to develop a dynamic integrated
web-based interactive learning environment, and resource center, emphasizing
biodefense education, and mass casualty incident preparedness at the local, state and
national level.*

Introductions and Overview:

Mission of CIMERC
End user instructions on use of Bio-Experts Discussion Forum
Student participation within the Bio-Experts Discussion Forum
How the Bio-Experts Discussion Forum translates to the development of the Biodefense
Education Forum on the CIMERC website.

Comments, Issues and Discussion:

Saving of effort and avoiding reinventing of the wheel.
Using experience and lessons learned to the fullest extent.
Dissemination of information attained through the use of the best practices approach.
Share working models and learning processes by which they were developed.
Share stories, situational successes and failures as related to the learning process.
Make available mutually beneficial information and experiences.
On demand access to information via the World Wide Web like libraries, rural maps and
expert advice.
Guidance on managing limited rural resources and personnel.
View of the "big picture" in a "Sim-City" style of on line services.
Hearing from and being able to interact with diverse group of experts.
Pool rural purchasing power.
Provide a one-stop-shopping website to get information quickly and easily.
Streaming focused real time information to the rural areas.
Contextualizing, Home Land Security (national) intelligence so that it is meaningful to
the local rural communities.
Providing a conduit for local communities to contact or interact with state and federal
agencies when issues arise in their rural areas and questions or issues need
addressing. Control of over reaction to national reports by the local public.

Scaling down or tailoring information.
Customized reports for different geographical areas broken out by roles of responsibly.
Extracting or templating customized reports.
Eliminate redundant information.
Centralized and standardized training and education process for all levels of medical and non-medical personnel.

What role does a "rural member" play in building the virtual community?

Consumers

Consumers provide information about what they care about, based on what they use on a regular basis. Patterns formed by users and a rating system help rate the effectiveness of what they found, how they found it and was is useful. This feedback proves helpful by leading to improved layout, content and access pathways.

Discussants

Hearing what you need and being able to articulate an answer or resolution. Creating a shared ethos, for open and honest progressive thinking and interaction. Not being afraid of operating in a virtual space. Understanding at many levels of discussions and being about to think out loud about a trick situation or problem in a safe comfortable web space.

Mentors/Experts

Qualified individuals with unique perspectives. Willing to share expertise within the virtual web space. Leaders and educators who are motivated to share knowledge for the betterment of others.

Authors

Writers of publications, documents, policies, procedures and guidelines.

Advisors

Providers of recommendations, answers, feedback. Ultimately giving directions to find the appropriate resources, mentors or experts "I am not sure, but I know someone who does"

THE NATIONAL BIOTERRORISM CIVILIAN MEDICAL RESPONSE CENTER (CIMERC) RURAL BIO-EXPERTS FORUM MEETING
24 FEBRUARY 2004
At
Saint Francis University's Center of Excellence For Remote and Medically Under-Served Areas (CERMUSA), Loretto Pennsylvania

Introduction:

On 24 of February 2004, the National Bioterrorism Civilian Medial Response Center (CIMERC) conducted the second in a series of Rural Experts meetings on the campus of Saint Francis University, Loretto PA. This meeting was offered as a live meeting on location and also virtually via the CIMERC "Discussion Forum". Many members of the local healthcare community were in attendance. This group included but not limited to persons representing the following disciplines: Hospital emergency preparedness, emergency medical services, military, regional emergency medical services, hospital safety/security, medical education, bio/chemical detection, and members of both the rural and urban CIMERC programs.

Meeting Agenda:

- Virtual Community benefits as a communication and education tool
- CIMERC Forum progress since November 2003 meeting
  - o FAQ
  - o Ask The Expert
  - o Problem Simulation
  - o Discussion Forum
  - o Informatics Database
- Define community security needs and access control to forum tools
- Evaluate and define forum structure for optimal performance
- Determine additional needs and functionality to enhance the community environment and interface

Outcomes Achieved:

Based on input from the collective group of rural experts in person and virtually the following outcomes were achieved.

- Defined the dynamics of the civilian medial emergency response community
- Identified additional content for state profiles
- Reached consensus on what "security" really means to community participants
- Identified experts and expertise for discussion forum and ask the expert
- Identified education and course content leading to con-ed for healthcare providers as a high priority
- Defined specific look and feel traits which would be beneficial and enhanced the user interface experience while working in the discussion forum

- Collected many suggestions for process and content improvement of CIMERC site to include:
  - o Using a rating system for participants and content
  - o Increase the educational content of the web site
  - o Courses which carry CME, CEU, Con-Ed and Certifications
  - o Individualized "forum spaces" for small group interaction
  - o Explore collaborative partnerships to support this monumental effort
  - o On-line courses and CD ROM courses
  - o Dial up connectivity and content on web site

APPENDIX R5

CONTACT INFORMATION FOR DISTRIBUTED LAPTOPS

Laptops were issued to the following;

▲ Patti DeFrehn
Director of Trauma Services
Memorial Medical Center
1086 Franklin Street
Johnstown, PA 15905
(814) 534-9000

▲ Steven Benza
Director of Safety
Windber Medical Center
600 Somerset Avenue
Windber PA 15963
(814) 467-6611

▲ Donald Toma
Director Pre-hospital Services
Jeannette District Memorial Hospital
600 Jefferson Avenue
Jeannette PA 15644
(724) 527-9341

▲ Dr. Thomas Gessner
Medical Director
Latrobe Area Hospital
121 West Second Avenue
Latrobe PA 15650-1096
(724) 537-1000

▲ Mary L. Libengood
President
Meyersdale Medical Center
200 Hospital Drive
Meyersdale PA 15552
(814) 634-5911

▲ Dr. Samuel E. Long
Director of Emergency Services
Miners Hospital
290 Haida Avenue
PO Box 689
Hastings, PA 16646
(814) 247-3100

▲ Dr. Rod Grooms
Director of Emergency Services
Armstrong Memorial Hospital
One Nolte Drive
Kittanning PA 16201
(724) 543-8500

Distance learning courses offered through the National Bioterrorism Civilian Medical Response Center's (CIMERC) website (www.cimerc.org).

▲ **Emergency Responses to Terrorism Self-Study Guide:**

Sponsor:	USFA National Emergency Training Center
Author:	Federal Emergency Management Agency (FEMA) and The U.S. Fire Administration
Format:	PDF
Publication:	1999 (Rev.) 2002
Description:	This self-study course is designed to provide the reader with a general introduction to the basic concepts for first-responder awareness at the scene of a potential terrorist incident. This course is a training companion to the NFA's course, Emergency Response to Terrorism: Basic Concepts (ERT:BC).

▲ **Medical Management of Radiological Casualties Handbook:**

Sponsor:	United States Army
Author:	Military Medical Operations Office Armed Forces Radiobiology Research Institute
Format:	Text
Publication:	1st Edition, 1999
Description:	The purpose of this handbook is to provide concise supplemental reading material for the Medical Effects of Ionizing Radiation Course, which is the only course in the Department of Defense for training health care professionals in the management of uncontrolled ionizing radiation exposure.

▲ **Medical Management of Biological Casualties Handbook:**

Sponsor:	United States Army
Author:	US Army Medical Research Institute of Chemical Defense
Format:	Text
Publication:	4th Edition, 2001
Description:	The purpose of this text is to serve as a reference for the health care provider on the front lines, whether on the battlefield or in a clinic, who needs basic summary and treatment information quickly.

▲ Medical Aspects of Chemical and Biological Warfare:

 Sponsor: United States Army
 Author: Borden Institute, Walter Reed Army Medical Center
 Format: PDF
 Publication: 2002
 Description: This volume was prepared for military medical educational use. The focus of the information is to foster discussion that may form the basis of doctrine and policy. The volume does not constitute official policy of the United States Department of Defense.

▲ Are We Ready? A Guide to Citizen Preparedness:

 Sponsor: Community Emergency Response Team (CERT)
 Author: Federal Emergency Management Agency (FEMA)
 Format: PDF
 Publication: 2002
 Description: This document integrates facts on disaster survival techniques, disaster-specific information, and how to prepare for and respond to both natural and man-made disasters. It is intended for helping individuals prepare themselves and their families for disasters. Are You Ready? provides a step-by-step outline on how to prepare a disaster supply kit, emergency planning for people with disabilities, how to locate and evacuate to a shelter, and even contingency planning for family pets. Man-made threats from hazardous materials and terrorism are also treated in detail. The guide details opportunities for every citizen to become involved in safeguarding their neighbors and communities through FEMA's Citizen Corps.

▲ Weaponized Chemical Agents Video Training:

 Sponsor: United States Navy
 Author: Bureau of Medicine and Surgery
 Format: QuickTime and Real Player
 Publication: 2003
 Description: Sponsored by the Department of Navy as a test, web-based education site containing a collection of short audio/video tutorials compiled by Depratment of Defense physicians. These videos cover a wide range of medical tools and techniques to diagnos a patient who presents with a suspected illness. These cases are addressed in a simulated clinical setting as well as in the field environment. Each scenario offers medical insight by demonstrating common clinical signs and symptoms of patients as they relate to weaponized and non-weaponized nuclear, biological, and chemical agents.

APPENDIX R7

CIMERC WEB SUMMARY DATA

CIMERC Web Site Tools and Traffic Data Information
Data collection period 14 July 2003 through – 04 November 2003

Unique Visitors	12,407
Total Web Site Hits	63,689
Homepage Hits Average per day	110
Webpage Views Average per day	517
Unique Visitors Average per day	190
Strategies for Incident Preparedness	5,173 Downloads
Hospital Preparedness Self Assessment Tool	1,728 Completed
News Page	10,080
Events Page	1,185
Education Page	2,086
Traffic Patterns on Web Site	Weekend (5.1%),
Weekdays (94.9%)	

Web Browser Use	
Microsoft IE 6.0	47,747
Microsoft IE 5.5	6,847
Microsoft IE 5.0	1,792
Microsoft IE 5.01	1,285
Others	946

Operating Systems	
Windows 2000	27,295
Windows NT 5x	21,295
Windows NT 4.0	1,840
Windows 98	4,739
Windows NT	529
Macintosh Power PC	261
Others	800

CIMERC PRODUCTION
WEB SERVICES DESIGN

Richard Joltes, Consultant
April 19, 2003

Preface

Successful implementation of a production-level computing service or software application requires a great deal of forethought and planning in the areas of supportability, security, usability, reliability, scalability, and redundancy. For instance, while it is technically simple to set up and implement a basic Web server under any hardware/OS combination (e.g., Windows/IIS, UNIX/Apache, Linux/Apache, etc.), it is much more difficult to design a solution that will satisfy the requirements of a production environment. Unlike an in-development or even an internal workgroup scenario, a production service will be used by an unknown number of frequently anonymous users whose actions cannot be predicted or controlled with any accuracy. These users become customers, who will "vote with their mice" if the service proves unreliable, unusable, or insufficiently useful for their needs. It is also a given that they will attempt to utilize components of the service in a manner never foreseen by the development team, and will uncover defects and security flaws in areas that were thought to be thoroughly tested in advance.

Some possible outcomes of an improperly planned or executed project are:

a) A product that is unusable due to overly complex or confusing User Interface (UI) design.

b) An inability to support the expected user base due to performance issues such as slow response time, program or Web site crashes, or insufficient network resources.

c) Theft of user data or other sensitive material

d) A product that does not meet the needs of the expected user community.

Each major area of concern can be expressed briefly as follows.

- *Supportability.* The infrastructure must be manageable from the standpoint of both hardware and software; highly customized or difficult to obtain components should be avoided wherever possible if comparable "off-the-shelf" alternatives are available. Customized or locally developed software must be adequately documented, with useful comments inserted into the code to allow future developers and support personnel to manage or maintain the code to address defects, new requirements, or other changes. A reliable source archive must be maintained, especially in the case of compiled code. Replacement hardware must be sufficiently generic or otherwise readily available; except in highly

specialized cases no more than 24 hours should be required to replace a failed component.

- *Security.* This encompasses physical, data, and operating requirements. The operating system and Web service should be sufficiently "hardened" to withstand basic Denial of Service (DoS) and other attacks, while live data must be protected via regular backup to some offline storage medium. Sensitive data that can be used to identify users or system personnel must be protected using appropriate password schemes, encryption where necessary, and other methods based on the sensitivity level of the information in question. Last, the physical environment where the machine(s) and networking gear are housed must be secured against intruders or even accidental access by legitimate employees.

- *Usability.* In order to be successful, software provided via the Web must be usable by any individual capable of starting a computer and gaining access to the Internet by modem or other means. This means that the user interface must be clear and concise, tool tips or other help sections must be provided, and the flow of information from URL to URL should be easy to understand. Forms should be simple to use and offer assistance to the user wherever confusion may occur. HTML must be generic, avoiding use of browser-specific tags or settings that will cause errors or unreadable pages for users who access the site using a browser other than that used when the site was developed.

  A corollary to the above is that the software offered should actually address the needs of the user base. It is impossible to develop effective software or tools for a given audience without first soliciting their input; if products are developed in such a vacuum it is very likely the result will be a service that no one uses. The input of the expected user base must be solicited early in the development cycle, and selected users should be given access to Beta versions of the Web site or application at regular intervals. Feedback is critical; the wrong time to find out that no one wants or needs a given application is after it has been released into the production environment.

- *Reliability.* Crashes, "hangs," and downtime must be avoided in the production environment. Site availability must approach 99.9% in order to avoid alienating members of the user community, who simply will go elsewhere if presented with error messages or long delays due to hardware or software failures. Uninterruptible Power Supply (UPS) hardware, PC or other servers equipped with dual power supplies, redundant disks and/or RAID arrays, redundant network links, and other measures that help boost reliability are mandatory in a production environment. The deployment of multiple physical servers, each handling a percentage of the overall load, should be considered. The term "single point of failure" must be kept in mind at all times when designing for reliability; in extreme cases it is even advisable to implement fully mirrored facilities in geographically dispersed locations though this is not presently deemed necessary in CIMERC's case.

- *Scalability.* The usage curve of production computing resources is never constant; in some cases, a particular server may sit nearly idle for an extended period before an event will cause it to become a more critical component in a production service. Access to the CIMERC Web site may remain consistently low until some external event (i.e. a terror attack) causes usage to increase dramatically. The service must be capable of handling such "usage spikes" without crashing or causing a noticeable degradation in response time. Additionally, the physical and data infrastructure should be designed so that new resources can be added as necessary to bolster the capabilities of the existing server farm.

- *Redundancy.* This has already been addressed to some degree, but it deserves special mention since even the fastest, most reliable server may crash or fail occasionally. Designing around a single powerful system may result in less reliable service than would be the case if numerous, cheap PCs were used. The rule "two or more of everything" should be followed wherever possible – network interfaces, disks, server systems, UPS support, and so forth – since redundancy provides measurable gains in performance, reliability, and scalability.

Caveats & Assumptions

Designing the physical CIMERC site infrastructure is difficult since no studies have been performed to adequately describe expected user profiles, usage curves, or software metrics. It is dangerous to assume that initial usage from outside the development team would remain low for some time after the "live" version becomes available; prior experience with Web-based resources shows that they may become saturated with requests almost immediately after being released to the public. Recently a "joke" Web site became so popular—despite zero advertising by its owners—that it achieved 4000 discrete "hits" *per second* over a sustained period, causing numerous server outages. This happened within days of the site going "live." While the CIMERC Web site is unlikely to see such a dramatic increase in usage, it is nevertheless prudent to be aware of the traffic level achieved by some sites on the Web.

It is also hazardous and inadvisable to design a solution to exactly fit specific expected requirements. Disk space, network bandwidth, or CPU usage requirements will increase over time; thus the initial solution should be able to handle a higher usage curve without the constant addition of memory, disk space, or other resources. Production resources should not be taken offline repeatedly in order to perform upgrades (as noted in the section on reliability) so it is always better to over-build somewhat.

Hardware

The following specification is offered as an initial recommendation for basic Web servers for this project. Again, note that we are currently using best-guess methodology to establish baseline parameters, and the actual requirements may vary from those outlined below.

A. *Server-class system (not a desktop workstation).*
   A server-class system is one that has been designed with expansion and reliability in mind. It places less emphasis on, for instance, graphics capability or

case design and more on areas such as power supplies, disk expansion slots or controllers, rack mount options, and hot swap capability. One should expect to pay roughly $3000 per system for a machine of this type.

B. *Dual power supplies, preferably hot swappable.*
Dual power supplies are designed to allow one unit to be serviced or replaced without requiring a system power-off or OS shutdown. This increases reliability and availability, and helps to minimize outages. Note that when dual supplies are in use, each should be plugged into outlets serviced by different circuit breakers, thus further enhancing reliability (if one breaker is tripped or fails, the other circuit takes up the load).

C. *RAID subsystem, 2 members per RAID unit, with an option for RAID 1/0 (mirroring/striping).*
RAID, or *Redundant Array of Independent Disks*, is a method of increasing both performance and availability in higher-end computing arrays. Since disk throughput is one of the primary factors affecting performance, distributing the workload across several "spindles" (disk units) helps speed up response time. Handled properly, RAID can also offer automatic fail-over for damaged disks as well as a convenient method for expanding storage without resorting to the creation of new partitions.

D. *Linux Operating System.*
Since Windows is not considered capable of serving the needs of a high-volume Web site, Linux is suggested as an inexpensive and robust alternative. Linux is based on the UNIX operating system that comprises the backbone of Internet services; it offers much better security and reliability than the Windows platform and is the OS of choice for all larger Web-services providers. A "professional" release of either SuSE or Red Hat Linux is available for under $100. More expensive "server" class packages are available, but these include more extensive software support contracts or hardware support for high-end systems (multi-CPU, multi-GB memory configurations) that are not yet needed for the CIMERC project. The OS should be installed and patched to the latest level prior to switching the existing CIMERC services to the Linux systems, since this will eliminate or minimize the need for downtime and upgrades for some time afterward.

E. *Service contract: 24 hours per day, 7 days per week, 365 days per year, (AKA "7 x 24 x 365") coverage.*
Since the production service must be highly available, a high-level, fast response, on-site service contract should be purchased to cover all server-class machines as well as any ancillary networking or other devices directly related to the daily operation of the server farm. In the case of networking hubs, UPS devices, or other common systems, it may be adequate to purchase a few back-up "cold spare" replacements that are *kept, unused, in a storage cabinet,* ready for immediate deployment in the eventuality that a failure occurs in the production environment.

F. *High-speed backup tape subsystem.*
Obviously, the data must be backed up on a regular basis. While much of the CIMERC site will become relatively static as components are completed and released into the production tree, backups must be taken on a regular basis to ensure that the most current files can be restored following a disk failure or other catastrophe. The exact specification of the backup device will depend on the amount of data involved: a CD-R can hold up to 660MB, while a DVD-R stores approximately 4GB per disc. Various tape-based solutions can hold upwards of 80GB per tape. Many higher end sites use DLT (Digital Linear Tape) systems that hold 40-80GB per tape; these products also offer the advantage of speed, since backups can be made at a rate of 4-5MB per second. The media are also re-usable, and the higher data density is useful in minimizing storage space requirements.

If databases of any type are involved in the final site, their contents must be backed up on a more frequent basis since the data contained within is likely to be more volatile than that found in the HTML tree.

An alternative backup solution might involve removable hard disks; these could be plugged into the server, a backup taken, and the disk removed for storage in a secure location. This option offers the advantage of speed and portability.

G. *UPS system for power protection.*
To increase reliability, UPS devices must be installed and configured to prevent minor power outages or voltage "sags" from crashing the servers. Integrated units that communicate with a power-management facility within the Linux OS should be used, since they will allow the systems to shut themselves down gracefully if the UPS batteries are drained before power is restored. This monitoring service should also be configured to notify system management personnel (via pager, telephone, etc.) when a power failure has occurred so that these personnel can respond appropriately to the situation.

Two (or more) server class systems should be purchased simultaneously in order to benefit from commonality of hardware and configuration; this will ease management and troubleshooting chores over the life of the machines.

Configuration

As noted earlier, single points of failure should be eliminated wherever possible in order to minimize downtime and help alleviate performance issues. To this end, it is suggested that the initial configuration of the Web service be composed of two physical systems, with the option for adding or modifying this arrangement as necessary. The procedure for doing so is as follows:

1) Each system will be assigned an "internal" IP (Internet Protocol) address and name, e.g. 'cm_prod_1.CIMERC.org,' 10.2.3.4 and cm_prod_2.CIMERC.org,' 10.2.3.5.

2) The URL 'http://www.CIMERC.org' will be re-defined so that each of the above IP addresses becomes an *alias* for the master address of 209.158.22.15. One can see an example of the appearance of such an alias by examining the DNS (Domain Name Service) entry for *www.ebay.com*:

Non-authoritative answer:
Name: pages.ebay.com
Addresses: 66.135.192.87, 66.135.192.88, 66.135.208.87, 66.135.208.88
Aliases: www.ebay.com

The effect of such a configuration (generally known as a "DNS round robin") is to spread user traffic across NN available machines; when a user attempts to access "http://www.ebay.com" he will be directed semi-randomly to one of the four IP addresses listed in the output above, thus assigning roughly 25% of the overall load to each of these machines. If a machine crashes or must be taken down for maintenance, it is a simple task to boot a replacement system to take its place. As an alternative, the DNS entry can be changed so that one machine is removed from the alias; the traffic on this machine is then monitored until all current user sessions have completed, at which time the system can be shut down. Likewise, if traffic increases and the addition of another server to the alias is desired, an administrator can simply configure a new machine and add its IP (perhaps 10.2.3.6 with host name cm_prod_3.CIMERC.org) to the alias.

Note that other, more elaborate alternatives (e.g. software such as IBM's *Network Dispatcher* or Linux "clustering" software such as *Beowulf*) are available to provide even more redundancy and automated fail-over of production services. At present the extra expense and complexity does not seem appropriate for the CIMERC project, though this situation may change in the future as the site's importance to the overall bio-terror response system increases.

3) In addition, individual UPS units (connected, as noted above, to separate circuit breakers) will be purchased and installed as needed. Critical ancillary equipment such as network hubs, routers, or switches should be connected to additional UPS units in order to protect them from unplanned outages or power-related issues. If desired, one large facility-sized UPS system could be obtained and placed into service to provide both power conditioning and outage protection for all components housed within the server room. Note that any UPS should be sized appropriately, and should be capable of providing backup power to the servers and other equipment for at least 30 minutes.

4) If possible, a redundant or secondary link to the Internet should be acquired so that traffic can be spread across >1 access point. If this is not possible or desired at present, a fast-response support contract must be negotiated with St. Francis' current network provider to ensure that outages are addressed in a timely manner. Again, such a contract must include coverage on a 7 x 24 x 365 basis, with a 4-hour or better response time guaranteed in the case of an outage.]

5) Since no high-end disk replication solution has yet been chosen, it is suggested that the release procedure from the test environment to the production one simply copy identical sets of files to a separate disk on each Web server. In this way, each server machine will be an exact duplicate of the other so that users will see identical material no matter which machine they are directed to. This solution should be revisited later, once workload and traffic have been profiled over time, to determine whether it represents an optimal means of synchronizing the server content.

6) To provide an alternate access point for management personnel in the case of a network failure or other problem, dial-in access via dedicated modems will be set up for each production server. This access will require additional passwords, or perhaps will be restricted to a narrow list of incoming telephone numbers, in order to maintain appropriate security.

7) If a database becomes a significant component of the CIMERC Web effort, this software should be installed on a separate production server in order to separate database processing from the basic Web/Apache services. Numerous options are available at no cost, e.g. mySQL, miniSQL, and so forth; otherwise, an appropriate license for a commercial product such as Oracle, DB2, or SQL Server should be purchased.

Implementation Timeline

Presently no project timeline is available for reference, so this document will propose one purely from a technical standpoint. The implementation of the proposed infrastructure is relatively simple and straightforward, but modifications may be necessitated by changes in the project's goals or deliverables.

- *May 5-9:* Create detailed specification for hardware (servers, hubs, UPS devices, etc.) and obtain vendor quotes.

- *By May 15:* Place hardware order with a selected vendor for delivery *no later than* 1 June.

- *June 2-20:* Install the selected Linux OS and patches, plus the Apache Web server and patches. Harden system by disabling any unnecessary services or accounts; add tripwire and other tools to monitor critical files. Allow systems to burn in to ensure the hardware itself is stable. Establish DNS round robin for testing purposes (using, perhaps, wwwdev.CIMERC.org).

- *June 23-30:* Copy HTML and other "live" files from the present www.CIMERC.org machine to the Linux systems. Have staff walk through the site URLs [note: also look for link-traversal tools to automate this process] to ensure that no broken links exist. Set up Apache log management tools, establishing automated weekly and monthly log reports and log file rotations.

- *July 7:* change the existing Windows machine's IP address so that it becomes w3.CIMERC.org (or w3dev.CIMERC.org). Simultaneously, alter the DNS round robin on the Linux servers so that www.CIMERC.org points to these systems. *From this point forward, the Linux boxes become sacrosanct and should not be*

altered or shut down unless absolutely necessary and sufficient precautions have been taken to minimize downtime. No development work whatsoever should take place on these systems.

- *July 8-31*: establish and test procedures for testing and migration of newly completed pages and tools from the development to the production environments.

From this point forward the technical aspect of the project will consist of refining monitoring and other tools, improvements to security and reliability, and advance planning for hardware upgrades that may be required as the project's scope expands.

Infrastructure Diagram
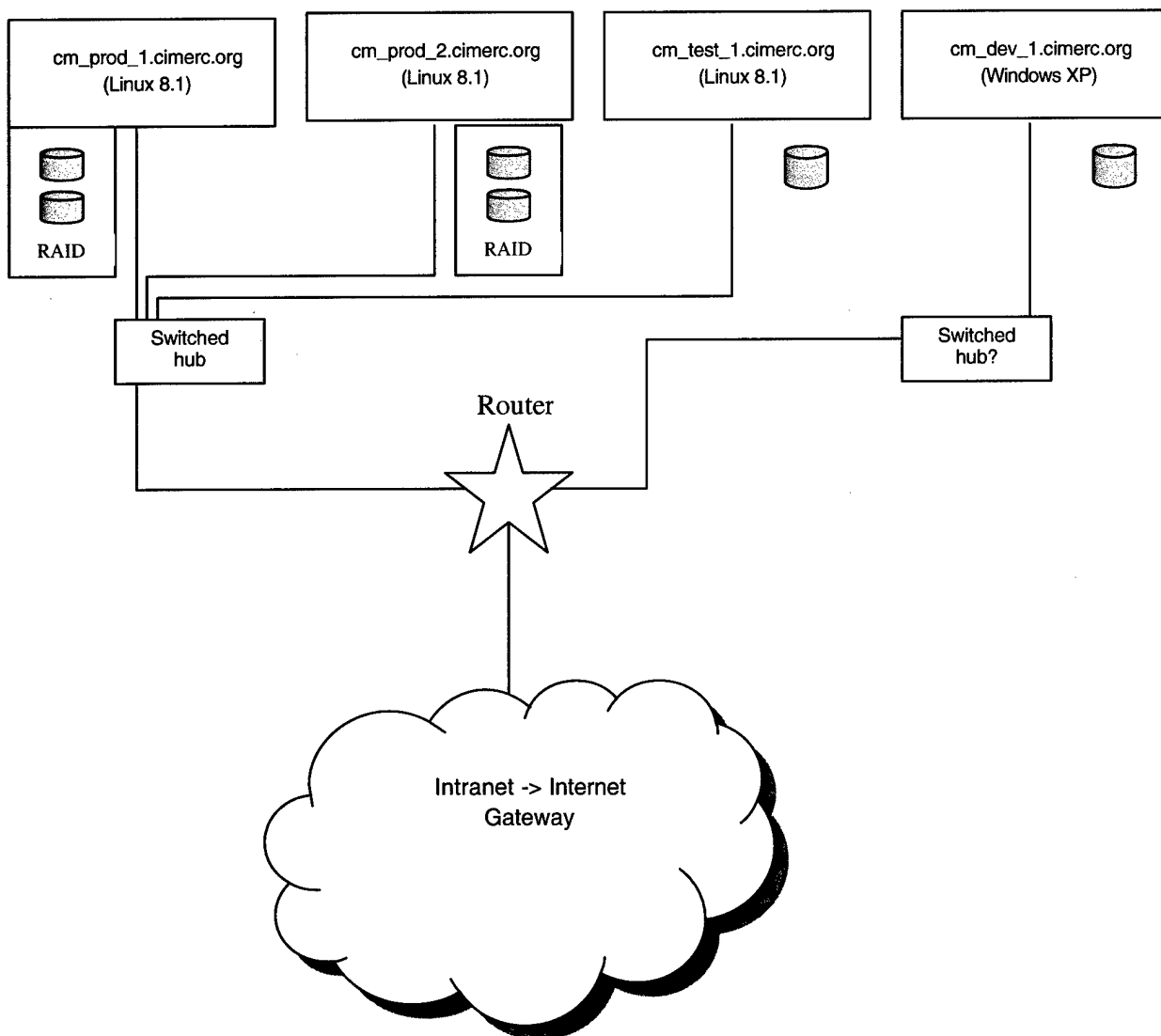
CIMERC PRODUCTION WEB SERVICES
STATUS REPORT AND FUTURE PLANNING

Richard Joltes, Consultant
December 5, 2003

Introduction

The CIMERC web service offering has improved significantly throughout the calendar year 2003, having been upgraded from a basic flat HTML proof-of-concept residing on a Windows based server to a more highly structured interactive environment using production grade Linux systems. This is in accordance with plans laid down in the last months of 2002, and reflects a growing awareness of the need for a stable, secure production environment. Further development of the security infrastructure is needed, but this is to be expected since rapid changes in software and methodology requires frequent audits and updates to all such services. See the *CIMERC Infrastructure Plan* (April 2003) for additional detail regarding pre-production planning and the basic tenets used to develop the system in its current form.

Hardware

New hardware was purchased in June 2003 specifically for use by the CIMERC Web service. It consisted of paired HP server-class systems with redundant power supplies, RAID arrays, and other features that will permit a higher level of availability than a standard desktop PC. Two servers were designated specifically for the Web service (Apache) while two others house the back-end Sybase database engine that provides a repository for the Bio Defense Forum. The paired systems are matched from a hardware standpoint in order to achieve commonality of components and ease of management.

As planned, Red Hat Linux was installed on these systems since its security features are considerably greater than those available under the Windows family of products. Version 9 was installed, along with all patches and utility updates available when the installation was performed. A regular schedule is being established to ensure that software patches, especially those salient to the security component of the system, are applied on a regular basis after first being tested on a non-production server.

Each production system is connected to a UPS (uninterruptible power supply) system in order to provide clean power and to protect against short-duration power outages or brownout conditions. The operating system monitors UPS and power status and will be set up to power down the systems automatically if conditions arise that require this action. However, the CERMUSA facility has its own back-up generator system; this feature should never be needed.

The St. Francis campus now has multiple connections to the Internet (one via Internet-2) in order to provide redundant access to the backbone. Each connection is provided by a different carrier. This eliminates single points of failure and increases reliability even further, since the failure of one link does not totally remove access to the CIMERC Web site.

Software

Various operating system options were selected during installation in order to enhance the security of the system as a whole. By installing the 'server' option, the Red Hat installer implemented a higher level of security than would be the case on a user workstation or login system; it mandates that various known points of attack are closed by default and must be explicitly opened by the system administrator.

Additionally, specific utilities were installed or enabled in order to enhance security even further. Briefly, the following standards have been established.

- All inbound Telnet has been disabled and replaced with ssh (secure shell), which encrypts all user sessions to prevent packet sniffing and other methods of obtaining passwords from network communications sessions.

- TFTP and other known insecure services are completely disabled.

- Repeated login failures will result in an account being locked and the activity logged (see below) by the syslog facility.

- 'Tripwire', SATAN, and other utilities have been installed to permit system surveys to be conducted on a regular basis to determine if intrusions or intrusion attempts have taken place.

- The syslog facility has been set up to monitor login activity and especially failures. The logs will be reviewed on at least a monthly basis in order to determine whether intrusion attempts have taken place.

- The sendmail facility, while enabled, has been set up to prevent relaying and other tactics commonly used by senders of "spam" messages.

- The ability exists to audit Web activity based on IP address range, file requests, and other metrics. This permits access patterns and activity levels to be monitored for security and performance purposes.

Operational Procedures

The production facilities are newly established and thus not all procedures are fully in place, but the following baseline has been established in order to maintain operational readiness and to monitor for malicious activity/potential hardware problems. This list will be expanded as operational experience is built up over time.

- A regular root password change schedule has been established. This password will be given solely to competent administrators who have an ongoing need for privileged access to the system. All other users' activities will be managed using group membership and access control software.

- Accounts will be created only for administrators and programmers; regular reviews will be performed in order to purge unnecessary accounts left behind by departed employees. In addition, any account owned by an employee who leaves the project will be disabled immediately upon their departure; the root password will be changed at the same time if necessary.

- The production systems will not be used for regular user sessions (e.g., e-mail, software development, or other activities). No compilers other than those necessary for normal Web and/or database operations will be present on the systems.

- A master backup of the base system will be taken once all initial updates are completed; this backup will be stored in a secure location in case data corruption or malicious activity results in a production outage. Additionally, regular "incremental" backups will be taken of changed files and active database tables so that user data or newly added files are not lost.

- Automated monitoring of various critical areas (e.g. disk errors, suspicious user activity, etc.) will be implemented using cron jobs and pagers, so that administrators can be alerted of possible problems on a 7/24/365 basis.

- Web and database access logs will be reviewed regularly to look for "bot" activity as well as intrusion or DoS (Denial of Service) attacks or attempted attacks.

- The production systems reside in a locked server room accessible only to administrators and security personnel. Access is controlled by a card key system that maintains tracking data at an off-site facility; this permits log reviews and other investigative procedures should a security breach occur.

Forward Planning

At present, only one database server and one Web/application server are in the production pool. Once CERMUSA's new building is fully on-line, the other two machines will become secondary/fail-over servers in order to provide redundant services in the event of a hardware failure, malicious event, or power problem at the main facility. This will also provide the foundation for a DNS round robin fail-over system (again, see the *CIMERC Infrastructure Planning* document for details) that will establish the ability to load-balance across the two systems.

Should the user load rise beyond all expectations, the presence of the DNS round robin will permit the addition of NN more servers to the pool, thus distributing processing across even more systems. As a bonus, the round robin will make the addition of more servers completely transparent to the user.

Once these two machines are enabled for production use, a procedure will be established to maintain a mirror status between the associated systems. The Web/applications servers will be kept in sync using an automated file-copy facility; the database servers will be linked using Sybase's built-in mirroring features. Once fully in place, this system will ensure data consistency across the machines so that any user session will see identical data and layout.

Final Comments

The overall objective is the development of a powerful, reliable, expandable set of services that can meet the needs of the currently small user base while establishing a framework for an expanded, highly available distributed service should this prove necessary in the future. Its initial twin-server incarnation provides enough raw

horsepower and disk space to accommodate additional loading without the need for more hardware, and the higher level of security offered by Linux is useful due to the potentially sensitive nature of the data. It should be remembered that this site is a component in the Homeland Defense infrastructure and therefore represents a potential target; though the likelihood of this occurring seems small, it must be taken into consideration.

It is generally difficult to plan the reaction users will have to a new service on the Web, but the current methodology also provides the ability to react with reasonable rapidity to sudden changes in user activity or requirements. Once the round robin is in place, servers can be added or removed from the pool at will, whether due to hardware issues, upgrade requirements, or other considerations.

The present security procedures are at least adequate and can be improved as CERMUSA's new facility becomes available. It will be advantageous to add a more granular, manageable method of access control to the Bio Defense Forum, since the software delivered by Math Forum offers little protection against a determined attack and is very basic in nature. Security procedures should be reviewed at least every six months to determine if changes are necessary.

APPENDIX R9

LETTERS OF SUPPORT
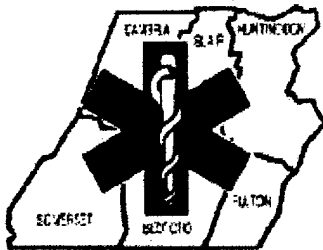
Southern Alleghenies E M S Council, Inc.

Olde Farm Office Centre • 1 Carriage House
Duncansville, Pennsylvania 16635
Phone: 814-696-3200 • Fax: 814-696-0101 • 1-800-EMSki-4U
Website: www.saems.com

December 12, 2003

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
PO Box 600
Loretto, PA 15632

Dear Mr. Silveira:

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities. We have been extremely pleased with the support and assistance provided by CIMERC in developing emergency medical response policy and preparedness tools. We encourage continued support of their fine work.

As you may know, an intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals to include local police, fire, emergency medical services and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that many local public agencies need planning, assessment, and implementation assistance and tools for training, and response programs that will assist the development of a coordinated event response. While we continue to prepare our personnel and equipment for the next mass casualty response, CIMERC continues to provide support and assistance and has truly become an additional resource to our program

I have worked with Mark Silveira, CIMERC's lead staff on rural development, and I can assure you of the high quality and thoroughness of their evidence-based and multi-stakeholder efforts. Please do not hesitate to contact me with any questions regarding their projects at (800)367-5448 or cmoen@saems.com.

Sincerely,

Carl L. Moen
Deputy Director

Chair, Medical Committee
South Central Mountains Terrorism Task Force.

Commissioners:
Fred L. Scisson, M.D., President
Ted Barnik
Kathy L. Holtzman
Executive Director
Michael H. Huss

Director of Communications 9-1-1:
Robbin J. Melnyk, ENP, PEM
Director of Emergency Management Agency:
Ronald J. Springer, PEM
Cambria Allegheny Regional Highway Safety Network:
Donald C. Druss, Project Coordinator

Cambria County
Department of Emergency Services

December 11, 2003

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
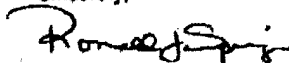P O Box 600
Loretto, PA 15940

Dear Rural Director,

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities. We have been extremely pleased with the leadership shown by CIMERC in developing emergency medical response and preparedness tools as well as policy. We encourage continued support of their fine work.

As you may know, an intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals to include local police, fire, emergency medical services and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that many local public agencies need planning, assessment, and implementation tools for training and response programs that will assist the development of a coordinated event response. While we continue to prepare our personnel and equipment for the next mass casualty response with limited resources, CIMERC continues to provide guidance and has truly become an additional resource to our program.

I have worked with Mark Silveira, CIMERC's lead staff on rural development, and I can assure you the high quality and thoroughness of their evidence-based and multi-stakeholder effort. Please do not hesitate to contact me with any questions regarding their projects at (814) 472-2050 or rspringer@co.cambria.pa.us.

Sincerely,

Ronald J. Springer
Director / Emergency Management

JEANNETTE DISTRICT
MEMORIAL HOSPITAL
600 Jefferson Avenue • Jeannette, PA 15644
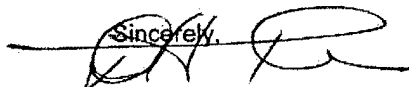(724)527-3551

December 10, 2003

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
PO Box 600
Loretto, PA 15632

Dear Mark,

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities. We have been extremely pleased with the leadership shown by CIMERC in developing emergency medical response and preparedness tools as well as policy. We encourage continued support of their fine work.

As you may know, an intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals to include local police, fire, emergency medical services and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that many local public agencies need planning, assessment, and implementation tools for training and response programs that will assist the development of a coordinated event response. While we continue to prepare our personnel and equipment for the next mass casualty response with limited resources, CIMERC continues to provide guidance and has truly become an additional resource to our program.

I have worked with Mark Silveira, CIMERC's lead staff on rural development, and I can assure you the high quality and thoroughness of their evidence-based and multi-stakeholder effort. Please do not hesitate to contact me with any questions regarding their projects at 724-527-9341 or dthoma@jdmh.org

Sincerely,

Donald H. Thoma
Coordinator Prehospital

Memorial Medical Center
Member Conemaugh Health System

December 11, 2003

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
PO Box 600
Loretto, PA 15632

Dear Rural Director,

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities. We have been extremely pleased with the leadership shown by CIMERC in developing emergency medical response and preparedness tools as well as policy. We encourage continued support of their fine work.

As you may know, an intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals to include local police, fire, emergency medical services and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that many local public agencies need planning, assessment, and implementation tools for training and response programs that will assist the development of a coordinated event response. While we continue to prepare our personnel and equipment for the next mass casualty response with limited resources, CIMERC continues to provide guidance and has truly become an additional resource to our program.

I have worked with Mark Silveira, CIMERC's lead staff on rural development, and I can assure you the high quality and thoroughness of their evidence-based and multi-stakeholder effort. Please do not hesitate to contact me with any questions regarding their projects at pdefreh@conemaugh.org.

Sincerely,

Patricia M. DeFrehn

Patricia M. DeFrehn, RN, BS, MBA, CEN
Director, Emergency/Trauma Services

Chairperson
Cambria-Somerset Disaster Management Taskforce

1066 Franklin Street
Johnstown, PA 15905-4398
814-534-9000
www.conemaugh.org

DEPARTMENT OF EMERGENCY SERVICES

County of Somerset
100 E. Union Street
Somerset, PA 15501

Phone: (814) 445-1515
FAX: (814) 443-1090
E-Mail: lohr@co.somerset.pa.us

Richard B. Lohr
Director   10 Dec 03

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
PO Box 600
Loretto, PA 15632

Dear Rural Director,

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities. We have been extremely pleased with the leadership shown by CIMERC in developing emergency medical response and preparedness tools as well as policy. We encourage continued support of their fine work.

As you may know, an intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals to include local police, fire, emergency medical services and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that many local public agencies need planning, assessment, and implementation tools for training and response programs that will assist the development of a coordinated event response. While we continue to prepare our personnel and equipment for the next mass casualty response with limited resources, CIMERC continues to provide guidance and has truly become an additional resource to our program.

I have worked with Mark Silveira, CIMERC's lead staff on rural development, and I can assure you the high quality and thoroughness of their evidence-based and multi-stakeholder effort. Please do not hesitate to contact me with any questions regarding their projects at (814) 445-1515 or shinholt@co.somerset.pa.us.

Sincerely,

Richard G. Shinholt
Somerset County Emergency Management
Deputy Coordinator
Planning/Training

USAMRMC Log No.: 02101001

R-51

Windber Medical Center
Member Conemaugh Health System

12/10/03

Mark Silveira
National Bioterrorism Civilian Medical Response Center (CIMERC)
Saint Francis University
PO Box 600
Loretto, PA 15632

Dear Rural Director,

Please accept this letter of support for the National Bioterrorism Civilian Medical Response Center's (CIMERC) efforts for biodefense development activities.

I had the pleasure of meeting with Mark in October of this year when he and Kristin Joltes traveled to our facility to bring us a laptop computer for use in our EOC and to explain the mission of CIMERC. I was impressed with his knowledge and presentation skills. We had a very productive discussion on Bioterrorism, Weapons of Mass Destruction, training and equipment needs. An intentional release of a biological agent or a natural biological epidemic would require a coordinated response effort by a variety of public agencies and hospitals along with local police, fire, EMS and public health. Nationwide studies by the National Association of City and County Health Officials (NACCHO) and other government agencies have revealed that a major weakness in emergency preparedness is that many local public agencies need planning, assessment, and implementation tools for training and response programs that will assist the development of a coordinated response to a major natural or manmade event.

This is especially true for rural areas in particular for smaller hospitals such as ours where we continue to struggle preparing our staff and equipment for the next mass casualty response with limited resources. We have been extremely pleased with the leadership shown by CIMERC in developing emergency medical response and preparedness tools as well as policy. Too often planning, policies and resources are tailored to fit the needs of large urban areas without much thought to the needs of rural areas, a "one size fits all" mentality. This may be fine for "hats" but is often detrimental in emergency preparedness planning for a true organized, coordinated national response. Thought must be given to the special needs of rural areas, such as limited manpower, resources, hilly terrain, remote locations, and all the other things unique to a rural environment versus a large urban area. CIMERC provides a unified "voice" for the rural community and their continued guidance and input has become an important resource to our emergency preparedness program. They have also become a resource for the Cambria/Somerset Disaster Management Task Force which is a multi-disciplinary group with representation from every hospital in Cambria and Somerset county as well as the 911 centers in both, Fire, EMS, Police and other public agency representation.

USAMRMC Log No.: 02101001

R-52

RURAL PRESENTATION

Rural Bioterrorism Response Network Prototype

Saint Francis University's Center of Excellence for Remote and Medically Under-Served Areas (CERMUSA), Loretto PA.

CiMeRC

Rural Bioterrorism Response Network Prototype

Rural Network Development: An Overview
Final Report

CiMeRC

Rural Bioterrorism Response Network Prototype

The Rural Network Development: An Overview
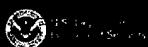
CDC

EMERGENCY MANAGEMENT

United States Department of Health & Human Services

CiMeRC

Rural Bioterrorism Response Network Prototype

Problem Statement
Approach
Methods
  • Rural Task Force
  • Rural Response Network
  • Rural Test Bed
Conclusion
Final Report

CiMeRC

Problem Statement

Nearly 73% of all emergency services staffed by volunteers

In the Commonwealth, an estimated 90% of the medical infrastructure is
:
:
:

CiMeRC

Problem Statement

Sufficient medical infrastructure, specific educational materials, individualized healthcare core training, and supportive infustructure to achieve minimal competency does not exist for most rural areas

Most major funding initiatives at the federal and state level are utilized to support preparedness efforts in major cities, and remain largely ineffective in reaching the rural, local level (Hall, 2003)

CiMeRC

Approach

Develop an effective and coordinated civilian medical response to a mass casualty incident, naturally occurring event, or man made accident.

Leverage existing infrastructure to
- .
- .
- .

CiMeRC

Methods
Rural Task Force

Composition: Local government agencies
Primary Function: Plan and coordinate resources covering two rural Pennsylvania Counties
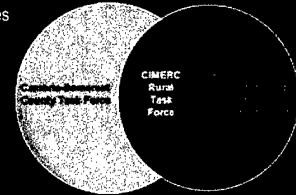
CiMeRC

Methods
Rural Task Force

Federal Emergency Management Agency (FEMA) Metropolitan Medical Response System (MMRS) Region 13 (bold border): A Geographic Comparison with Pennsylvania Emergency Management Agency (FEMA) Counter Terrorism Task Forces

Cambria-Somerset County Emergency Management Task Force (dashed border): A Geographic Comparison with the Federal Emergency Management Agency (FEMA) Metropolitan Medical Response System (MMRS) Region 13

CiMeRC

Methods
Response Network

Composition: county government agencies, local level departments and municipalities, senior leadership, and policy makers at each of the "test bed" sites/facilities
Primary Function:
- .
- .

The "Network" represents the communication and disaster management interoperability services aspect of the Rural Test Bed

CiMeRC

Rural Response Network

Western Pennsylvania Counties Represented in the Rural Response Network
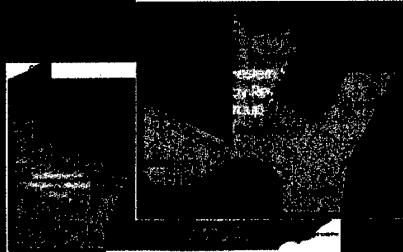
CiMeRC

Methods
Rural Test Bed

Composition:
Saint Francis University's Center Of Excellence For Remote and Medically Under-Served Areas
Cambria County 911, Assistant Director
Cambria SHARP/HAZMAT Team, Director
Memorial Medical Center, Director of Trauma Services Memorial Medical Center
Miners Medical Center, Director of Emergency Services, Miners Hospital
Windber Medical Center, Director of Safety Windber Medical Center
Latrobe Area Hospitals, Medical Director, Latrobe Area Hospital

CiMeRC

2

Methods
Rural Test Bed

Composition:
- Meyersdale Medical Center. President, Meyersdale Medical Center
- Armstrong County Memorial Hospital, Director of Emergency Services,
- Jeannette District Memorial Hospital, Pre-hospital Services Jeannette District Memorial Hospital
- Loretto Emergency Medical Services, Director
- University of Pittsburgh Public Health Center, Assistant Director
- Chem Image Co. Associate Director
- InSORS, Technology Group, President for Government Services

CiMeRC

Methods
Rural Test Bed

Primary Function:
- Contribute to the long term solution planning for rural preparedness.
- Bolster preparedness levels of the rural hospitals and emergency medical services.
- Provide continuous feedback and evaluation of the overall efforts of CIMERC as examined through the identified needs of the rural Test Bed.

CiMeRC

Methods
Rural Test Bed

Federal Emergency Management Agency (FEMA).
Metropolitan Medical Response System (MMRS) Region 13
(bold border): A Geographic Comparison with Pennsylvania
Emergency Management Agency (PEMA) Counter Terrorism Task Forces

CiMeRC

Conclusions

Results

- Evaluated medical facilities for mass casualty preparedness
- Developed the rural response network
- Created comprehensive biological / WMD training course

- Developed a multi-county preparedness communication plan

- Provided data to develop the Biodefense Education Forum
- Established baseline technology and infrastructure plan
- Established the rural experts group

CiMeRC

Conclusions

- Need continued infrastructure support to bridge the technology gap,
- Enable new strategies for real time informatics,
- Provide just in time education and training,
- Better prepare communities for response to major emergencies,
- Enhance local communication in the rural environment.

CiMeRC

Conclusions

A sound response to a given mass casualty incident (MCI) requires a well trained and resourceful workforce. CIMERC proposes education and policy based efforts in the Readiness and Response Training concentration area to bolster MCI readiness and response preparedness.

CIMERC continues to recognize the vast differences and unique needs of the nation's rural population

CiMeRC

Rural Network Development
Final Report

Recent terrorist actions against the United States have heightened awareness regarding the threat of Bioterrorism among both the Armed Forces and the civilian population. The rural civilian population has identified potential vulnerabilities that may be mitigated through the development of an improved Bioterrorism Response Network. Advanced off-the-shelf interactive web-based and distance learning technologies were incorporated with work products developed from a Task Force effort. These products were utilized to engage key stakeholders in multivariate processes for addressing identified vulnerabilities and presenting an effective biodefense response within remote and rural areas.

Click Here To View Entire Document

CiMeRC
National Bioterrorism Center Medical Response Corp

BIODEFENSE EDUCATION FORUM

Introduction and Background

Experience with first responders and key actors in planning and policy development has made clear the rapid evolution of information and knowledge about effective response to bioterrorism threats and incidents. In a context of significant change and somewhat independent, sector-specific educational and policy initiatives, there is a critical need for a platform that facilitates learning and assessment across involved communities. The educational agendas of responders necessitate a coordinated and informed decision-making process by colleagues, military, and other sponsoring government agencies. All agencies involved in a coordinated response need to know the state of understanding and preparedness, as well as have a platform for disseminating and guiding the development of new information and policies. It is important that a solution fit easily and in a compelling manner into the already full professional lives of key stakeholders in order to generate the data about what end users know, need to know, and are concerned with, as well as the contact hours and reflection that increase retention and knowledge development. For these reasons, a web-based education portal was planned to integrate assessment, information exchange, and knowledge-building communities that are critical for both the responder and for agencies charged with developing national capacity and effectiveness.

The National Bioterrorism Civilian Medical Response Center (CIMERC) was created to promote the development of an effective response by the civilian medical communities to the earliest stages of biological terrorist attacks through the use of advanced technologies that will coordinate efforts between civilian medical responders and local, state and federal governmental agencies. CIMERC proposed the creation of a dynamic and integrated web-based learning environment through the development of the Biodefense Education Forum (the Forum), a portal featuring: a hospital self-assessment instrument, the Biodefense Information Repository, and the Biodefense Response Professional's Learning Environment.

A core group of emerging leaders will drive the Forum, a virtual community comprised of facilitators, mentors, experts, and learners. The roles of community members will shift over time as learners become mentors, mentors become experts, mentors facilitate new mentor training, and experts in one area become learners in another field of expertise. Already, the nascent community includes rural and urban experts in the fields of EMS management, fire and law enforcement deployment, planning for weapons of mass destruction events, epidemiology, forensic pathology, emergency communication dispatch (911), military interagency planning for complex contingency operations, health education, distance learning and instructional design, internet community building, and flight nursing. Invited subject matter experts and educational delivery experts created the framework to develop and nurture this Biodefense community in its earliest stages. To accomplish this goal, they will lead face-to-face orientation and educational workshops, respond rapidly to questions, promote participant contributions in Ask An

Expert and Problem Simulation, organize and annotate material for ease of discovery, monitor and modify site design based on user requests and needs, and seed, participate in, and moderate discussions.

There are two ways to use the site. One may utilize the site as a Forum associate who has access to special "office" functions in order to perform duties such as facilitation, moderation, mentoring, resource cataloging and categorization, and user support. One may also use the site as a general participant who seeks information, wants to publish ideas, or would like to connect with other community members. While a given community member may interact with the site in either, or both manners, the views of the site are termed the "public view" and the "office view". The public view supports the participant in finding information and in contributing to community and knowledge building activities. The office view of the site is where the facilitation, moderation, Ask An Expert feedback, Problem Simulation feedback, cataloging and categorization, and webmaster functions take place.

Although the Forum was designed for use by multiple biodefense response communities to foster cross-community learning, the first phase of the project focused on the development of the forum for the civilian medical emergency response community. Members of the civilian medical emergency response community will be able to evaluate the readiness of an institution or facility to respond to bioterrorist attacks by using the hospital self-assessment instrument. Personnel will also use the Information Repository (the archives of all interactions of the communities, FAQs and the Document and Image Library) as well as the interactive services (i.e. Ask An Expert, Problem Simulation Answer and Mentoring, and Discussions) inherent in the Professional Learning Environment to build and maintain their competencies.

The Forum was built upon the proven positive effect of Drexel University's Math Forum experience. Created with over $5 million of investment by the National Science Foundation, the Math Forum is one of the most successful educational Internet applications (ScientificAmerican.com editors, 2002, Sci/Tech Web Awards 2002). For almost ten years, since before the introduction of the World Wide Web, the Math Forum has provided services to math students, teachers and parents, and has built a strong and growing community of online users. The Math Forum now comprises over 1.2 million pages of content, has an active user community of over 650,000 teachers and students, receives up to 9,000 queries a month to its Ask Dr. Math expert service, and has mentored up to 3,000 students per week through its Problem-of-the-Week mentoring service. During a period of time when educators are struggling to document the effectiveness of teaching methods and educational outcomes, the Math Forum has continually assessed the educational impacts of activities on the site and documented the proven impact on teaching and learning of the services that it provides.

The use of online learning communities has provided a scalable education program quickly reaching a very large audience and rapidly generating high quality content that is developed and delivered on an as-needed basis. This both enhances the educational and professional value to the end user and provides rich data about the state of the

domain and user population. (Renninger and Shumar, in press, Learning at and with The Math Forum) and (Shumar and Renninger, 2002, Sustaining Online Community: Learning and Participation at the Math Forum)

Purpose Statement

The central purpose of the Forum is to provide rapid development and dissemination of new information, policies, and assessments of preparedness concerning effective response to bioterrorism and other MCI events, along with corresponding knowledge remediation. The Forum, modeled after successful digital library and interactive learning services in use at the Math Forum, is the environment that will best foster and facilitate the exchanges necessary to meet the aforementioned goals.

The ability to continuously assess an institution's preparedness level is paramount when considering mass casualty scenarios. This integrated educational concept leverages information captured from the self-assessment or external training modules with the multifunctionality of the Forum to augment and improve bioterrorism readiness and response capabilities. Every participant in crisis response receives some level of training, whether it is in the field, on the web, or via traditional classroom methods. The Forum is a value-added, web-based educational system that interfaces with existing training modalities. This unique system contains a hospital self-assessment tool that evaluates trainee knowledge acquisition, and the Forum that corrects weaknesses through a training remediation process and provides an increased understanding of geographic challenges and cross-disciplinary issues involved in bioterrorism preparedness and response. This integrated system leads to continual skill assessment and customized training, resulting in the successful deployment of well-trained emergency response personnel.

Project Objectives

The CIMERC Biodefense Education Forum (the Forum) addresses several needs of the civilian medical emergency response community. Together the community leaders, expert mentors and users of the Forum will be able to:

1) evaluate response skills,
2) accelerate skill acquisition and maintain skill currency,
3) benefit from targeted information delivery, content and services that are based upon evolving user identity,
4) build a knowledge base through interactions, collaborations, and published content,
5) accelerate learning of local challenges, strategies and program effectiveness for the Forum sponsor and multi-level response units,
6) promote the interaction of diverse professional groups for inter-group learning.

The self-assessment instrument will attract users seeking to compare their preparation with existing standards and identify areas for additional education. It will also provide assessment data to sponsors, and drive the users into the information and education functions of the portal. From embedded help links in the self-assessment instrument or from questions a member of the civilian medical emergency response community may have following the evaluation, the user will have the opportunity to have a query answered by browsing or searching; frequently asked questions (FAQs), discussion threads, the library of resources, or by asking an expert. Discussion groups, the Library of Resources, FAQs, and the Ask An Expert service will also be available directly through entry to the Forum. These services as well as a mentored Problem Simulation program will promote the generation of new content based on the interaction of individuals and community usage. CIMERC will expedite and encourage community building in the Forum by mentoring in the Ask An Expert, Problem Simulation, and Discussions services. CIMERC will increase the knowledge base by monitoring and cataloging relevant and exemplary material from the Forum's interactive services and including references to other notable resources in the library.

Keeping both user and sponsor learning in mind, the first year of the project has focused on software development and building the structure of the public and office segments of the Biodefense Education Forum. Implementation of site design and of educational principles for the fostering of cross-community exchange has been a priority. The initial focus of content and community development will be for the civilian medical emergency response community.

Demonstration of the Need

In the military's employment of an "anytime, anywhere" strategy in distance education and training, the Biodefense Education Forum supplements and enhances that effort through a web-based collaborative, learning environment. In an online community, the participants construct their own knowledge while building a knowledge resource for the entire community. The Forum initiates the constructivist-learning paradigm in the biodefense knowledge domain, providing an alternative to traditional distance education, course centered models. Even in discussions of online communities in literature on military distance learning, the research construct builds on an assumption of virtual community within an online course.

> "As student-centered activities are increasingly facilitated by emerging technology, the role of the faculty member or instructor shifts to facilitator, coach, or mentor who provides leadership and wisdom in guiding student learning." (Bonk and Wisher, 2000, p. 18)

The Forum is a permanent online community, outside of the strictures of a single course. The Forum actively promotes roles of facilitator and mentor, but the instructor does not assume those functions. In the Forum, experts and leaders emerge from the community itself, assisting the designers and Forum staff in creating the community's shape and bounds. The roles of learner, facilitator, mentor, and subject matter expert

are not static, with a community member playing one role in a particular interaction and functioning and another role in a second interaction.

Learning in an online community complements the learning, taking place in a directed environment by encouraging creative exploration of knowledge by fostering connections with other practitioners and resources. The virtual community supplements traditional learning methods with the environment's promotion of rapid and motivated skill acquisition and of improved knowledge retention. Just-in-time learning provides an example, demonstrating the long-lasting effect of information acquired to fulfill an immediate, specific need. The self-directed, mutual, and reciprocal exchanges enhance the focus and quality of the relationship to the subject matter and to one's fellow community member. In contrast with traditional distance learning environments, whose strength is in the transmission and retrieval of a pre-set curriculum, the Forum supports **learning driven by "question and explanation,"** a type of learning targeted to the development of higher order thinking and problem solving.

Methods

Technical Development

As with any software development process, one assesses project requirements, determines budgetary parameters, and narrows the methodology for meeting requirements dependent on budget and on existing resource. Developing and implementing this project required examination of client requirements for capacity and growth, maintainability, site functionality, security, and budget. With these factors in mind, project planning and execution focused on six building blocks: 1) re-utilization of core Math Forum software, 2) maintainability of selected hardware and software platform, 3) a viable upgrade path for the infrastructure, 4) system performance, 5) software developers' familiarity with the tools, and 6) time constraints inherent in the initial phase of the project.

Engineers built the core Math Forum software over a ten-year period with several different toolsets. The most recent, most adaptable, and most easily maintained Math Forum code is the foundation for the Biodefense Education Forum software. The Math Forum's "Nonpareil" discussion software was extended to add features for Biodefense Education Forum discussions. In addition, this software was utilized as the foundation for building new Ask An Expert and Problem Simulation software to best match user requirements and to have a single code base for all major Forum services.

The Forum technical team developed the applications software for ease of maintenance and to facilitate rapid development and deployment of the software. Applications development time was truncated due to an extended period of systems analysis, requirements identification, and the added responsibility of building the servers.

The applications software development strategy implied several choices in platform. "Nonpareil" discussion software was developed using Red Hat Linux, Perl, Mod_Perl, Mason, Apache, Glimpse and Sybase. Unfortunately, the versions of Red Hat Linux,

Perl, Mod Perl, Mason, Apache and Sybase were not the most recent versions. As a result, the technical team ported and tested the applications software code to run on the most current version and new development occurred under the new infrastructure platform. Porting of software from Red Hat 7 to Red Hat Enterprise 2.1 and porting of code from Sybase Adaptive Server Enterprise from 11.9.2 to 12.5 were necessary for the following reasons:

- ▲ Red Hat Linux 7 is no longer supported by Red Hat.
- ▲ Red Hat Linux, Enterprise Version, has five year guaranteed errata (as opposed to 1 year for the consumer versions).
- ▲ Complete annual operating system upgrades are necessary to continue receiving errata if a consumer version is selected
- ▲ The Enterprise version is supported by third parties such as Sybase and Oracle, as they have slower release cycles.

Sybase's Adaptive Server Enterprise 11.9.2 is no longer a supported version. Both of the older Linux and Sybase versions discontinued support in 2003. Sybase was selected over Oracle and PostgreSQL for ease of porting the "Nonpareil" software. Software Engineer analysis showed that porting to an upgraded version of Sybase would be quicker and more reliable than converting to Oracle or PostgreSQL. Initially, the technical team considered four options for the database platform: Sybase, Oracle, PostgreSQL, and MySQL.

Though the Linux community frequently uses MySQL, data integrity questions and capacity constraints eliminated it. PostgreSQL integrates into Red Hat Linux more efficiently, with a single point of support; however, future capacity constraints and the potential of difficulties in application software porting precluded this choice. While Oracle is the most fully featured database platform, with the greatest performance and capacity capability, the negative factors outweighed the positive. Impediments to using Oracle were the need for dedicated database administration resources for installing and maintaining Oracle and the potential of difficulties in application software porting. Consequently, Math Forum staff selected Sybase due to ease of porting, staff familiarity, and capacity greater than either Open Source platform (MySQL or PostgreSQL) offers.

CIMERC staff, in consult with technical staff at the Math Forum, selected server hardware for a combination of performance considerations and ease of software development. Compatibility challenges between existing software and new hardware added another layer of complexity to the software delivery process and necessitated some re-planning of platform selections.

Uncertainty over private versus public use of the Forum influenced capacity planning, a debate that remains open. Therefore, the need to meet three scenarios influenced capacity and security planning. These scenarios are: 1) an entirely private site, 2) an entirely public site, or 3) a site that allowed the combination of the two. Capacity was measured against the Math Forum site itself: a community that has taken ten years to grow. The Math Forum currently receives more than 650,000 unique visitors per month.

Queries are much simplified over Math Forum queries, the number of resources is much more limited, and the number of recorded interactions will take years to build. The Forum capacity is more than adequate for the near future. Additional capacity, without software modifications, may be achieved by hardware upgrade or increasing the number of Sybase database engines (through purchasing additional licenses). Software modifications may be necessary for hardware upgrades if there are compatibility issues with present infrastructure platforms. Additionally upgrading to a larger capacity database platform (e.g., Oracle) if desired, will require porting and testing of applications software.

The Forum addressed security on four levels: 1) physical, 2) network, 3) system level and 4) application software. CIMERC staff provided physical and network security, while the Math Forum implemented system level and applications software security and planned for future applications security. The debate over hosting a forum that is private, public or combination of both, challenged this process. In addition, security development presented the additional challenge of being a process in the making.

Deliberation continues on how to authenticate and how to implement public and private site passwords. If implemented, a group password will be assigned by a Web Master/Forum Administrator who will authenticate an individual requesting access (a policy decision allowing the individual to disseminate the password to his or her organization is forthcoming). Use or non-use of a password for the public portion of the site can be easily modified. Areas designated as private (e.g., expert discussions, Ask An Expert response and problem simulation response) will require the use of a password for access to a given component. However, areas designated as public (e.g., public discussion moderation) will not require a password.

System level security planning included creating a packet filtering firewall, DoS protection, password file definition, and turning off all unnecessary services.

Community Development

The experience of The Math Forum at Drexel University has served as a guide and model for online knowledge-building community development. This environment was developed in response to the need for an informal educational experience that complements more formal schooling and certification training, which is more formal. It takes advantage of the strengths of the Internet that permits one to bridge disparate communities through interactive services that enable users to help each other. In recording and reorganizing the interactions, one is able to build a knowledge base while simultaneously honoring member's contributions and making it possible for the community to see and reflect on its activity. This process developed a foundation for cultivating leadership, responsibility, and direction from within the community (Renninger and Shumar, 2002).

The key to building a successful knowledge community is a balancing act of seeding the community with resources and stimulating experiences, while nurturing the activity and

initiatives of the members. The success of the community hinges on the quality and extent of the members' largely voluntary contributions, which in turn depends on their perception that this environment has been built for and with others like themselves. In addition, the newness of this work space requires the captivation of the imagination of the early adopters. The early adopters must envision and embrace the Forum's possibilities and view the Forum as both responsive and resourceful. Thus, permitting them to overcome the critical threshold between disengagement and the willingness to surmount the learning curve. However, especially when encountering a new work space, it is also important that the imagination of the early adopters be sparked to see the possibilities and that it appear responsive and resourceful to the degree necessary to warrant climbing the learning curve and making space in one's schedule.

For these reasons, CIMERC initiated the Biodefense community building process by facilitating both face-to-face and virtual meetings with identified leaders in the civilian medical emergency response community. The underlying goals of the subject matter expert (SME) meetings were to:

1) Teach and advance skills in use of Internet technologies and introduce resources through exercising skills that are useful and interesting to them for their jobs or professional development.

2) Observe and discuss online activity and goals of SME's in order to identify programs that will serve these leaders and their colleagues, and identify the emerging SME group leaders who would be appropriate for extended support and cultivation as facilitators or developers of these programs.

3) Build a community with a strong sense of reciprocity, a resourceful and generous network of associates who provide help and share materials.

4) Help SME's create new resources and interactive services and in the course of this experience, develop technology skills that they could take back to the job, contribute to the resources available to everyone, and build momentum toward the more permanent community functions that would live beyond the initial gatherings.

In the context of these meetings, models and program ideas were utilized based on prior experience. The Math Forum and other online educational communities have identified three basic needs driving a learning activity to: 1) acquire help, 2) find something challenging and interesting to do, and 3) retrieve resources for one's work. The working hypothesis is that the Biodefense Education Community will exhibit similar characteristics although the relative priority of these functions and their specific attributes may vary significantly. Thus, mockups and initial discussions focused on functions such as Ask An Expert, Biodefense Case Studies, and the Biodefense Community Library.

Four meetings were planned to elicit interest and participation from subject matter groups from urban and rural areas. The meetings were conducted in a collaborative, resourceful, intense, inclusive, mutually beneficial, and self-directed way. The objective was to engage participants as motivated individuals and to identify potential leaders for the community. Coordinators shared background details and informative documentation regarding this effort with participants prior to all meetings.

1) The first part of the meeting was an introduction to all participants, to establish a collaborative spirit and to spark individual interests that may drive program development.

2) Next, each participant provided a virtual introduction of him or herself using the Biodefense Discussion Forum. Participants disclosed their background and current professional work related to the proposed Forum. The following two threads were initiated to stimulate additional discussion: "My Favorite Resources" and "What's Needed."

3) The session facilitator led the group through a tour of the different kinds of existing Internet resources and discussions. A strength and weakness discussion of reviewed resources and sites envisioned.

4) Participants brainstormed needs and services, building off the introductions and the tour. SME's identified relevant programs and resources that could be enhanced and leveraged for the purpose of emergency response and planning.

5) Small working groups prioritized projects within emerging categories, developed more detailed descriptions of the proposed service or materials, identified people and resources that should be involved, and possible non-technical next steps. The notes were posted in the Forum Planning area.

<u>Results</u>

Technical

Critical to the technical status is the state of the infrastructure (the server and applications platform status), the security measures implemented, and the applications software requirements that have been met.

Two servers were built from scratch, using Red Hat Linux, Perl, Mod_Perl, Mason, Apache, Glimpse and Sybase. The specific platform needed to be changed several times depending on hardware compatibility issues; applications software development requirements and systems level software compatibility issues. In the end, the platform for the Forum website consisted of Red Hat Enterprise Linux 2.1, Perl (bundled as part of Red Hat Enterprise), Mod_Perl 1.28, Mason 1.23, Apache 1.3.28, Sybase Adaptive Server Enterprise 12.5, and the latest version of Glimpse.

The online version of application server and database server creation and installation documentation are available at the following locations:
http://www.cimerc.org/office/manual/html/InstallApplication.html and
http://www.cimerc.org/office/manual/html/InstallationDB.html.
This information may also be found in the technical documentation in Appendix C.

Site capacity, given software platform, database, and applications software constraints, will provide more than the capacity available for the Math Forum site itself. As stated earlier in this document, the Math Forum currently supports a community of more than 400,000 members who make an average of greater than 2.5 visits per month. In addition, the Math Forum receives more than 650,000 unique visitors per month. Resource queries for the Biodefense Education Forum are much simplified over Math Forum queries, the number of resources is much more limited, and the number of recorded interactions will take years to build.

Security was addressed at both the system and applications level. Security implementation was carried out at the system level by creating a packet filtering firewall, DoS protection, password file definition, and turning off all unnecessary services. The packet filtering firewall opens SMTP(sendmail), HTTP(apache), SSH, DNS(domain), and Sybase ports on the application server and opens SSH, DNS, and Sybase ports on the database server, accepting all local traffic, and rejecting all other input. Password constraints were activated for length, lifetime of use, and dictionary checking. All unnecessary services were turned off as recorded in the /sbin/chkconfig/ file.

For implementation of applications security, the public and administrative portions of the Forum have separate passwords. The functions are segregated with completely separate views of discussion, expert, and problem threads. Additionally, experts and moderators may hold private discussions that are closed to the general public. With the launch of the site being imminent, there are two conflicting forces with polar security requirements. The effective building of community requires an easily accessible and

open portal, while the requirements of some in the Biodefense Expert Community require private and secured discussions. The solution will provide a discrete and private area for expert discussions and moderation considerations while providing a second area for public discussion. However, access to either area of the site will require the use of a group password. This paradigm is an explicit concern of the community builders.

The online version of the security setup documentation may be found at
http://www.cimerc.org/office/manual/html/SecuritySetup.html
This information may also be found in the technical documentation in Appendix C.

Applications software delivery was executed as per expected requirements. Descriptions of the work and sample screens are provided on the following pages for all services.

The Forum site was built with the delivery of core Education Forum services being paramount. On the home page, one may see the template, as it will appear on all pages of the site. Core services are listed on the menu bar. The content in the center of the page is completely flexible from one service and/or web page to another.
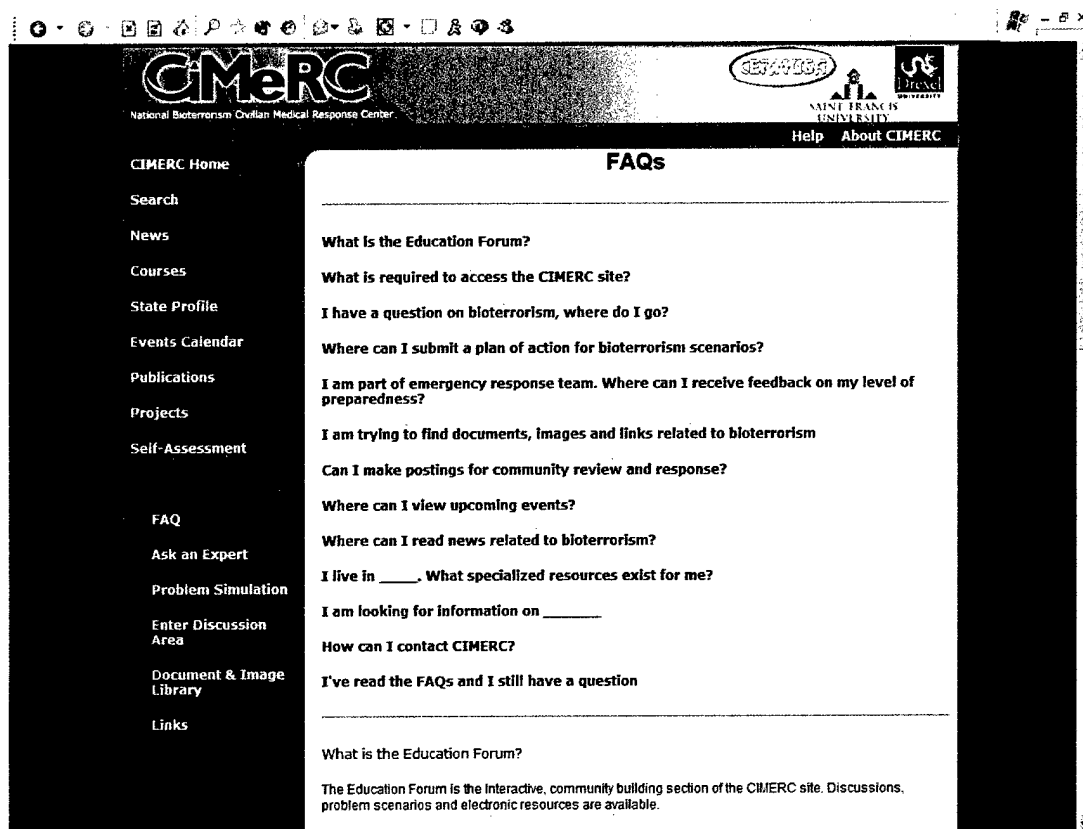
Figure 1. Screenshot of the Biodefense Education Forum (Forum) homepage. Core services are detailed along the left vertical column and page content is located in the center of the screen.
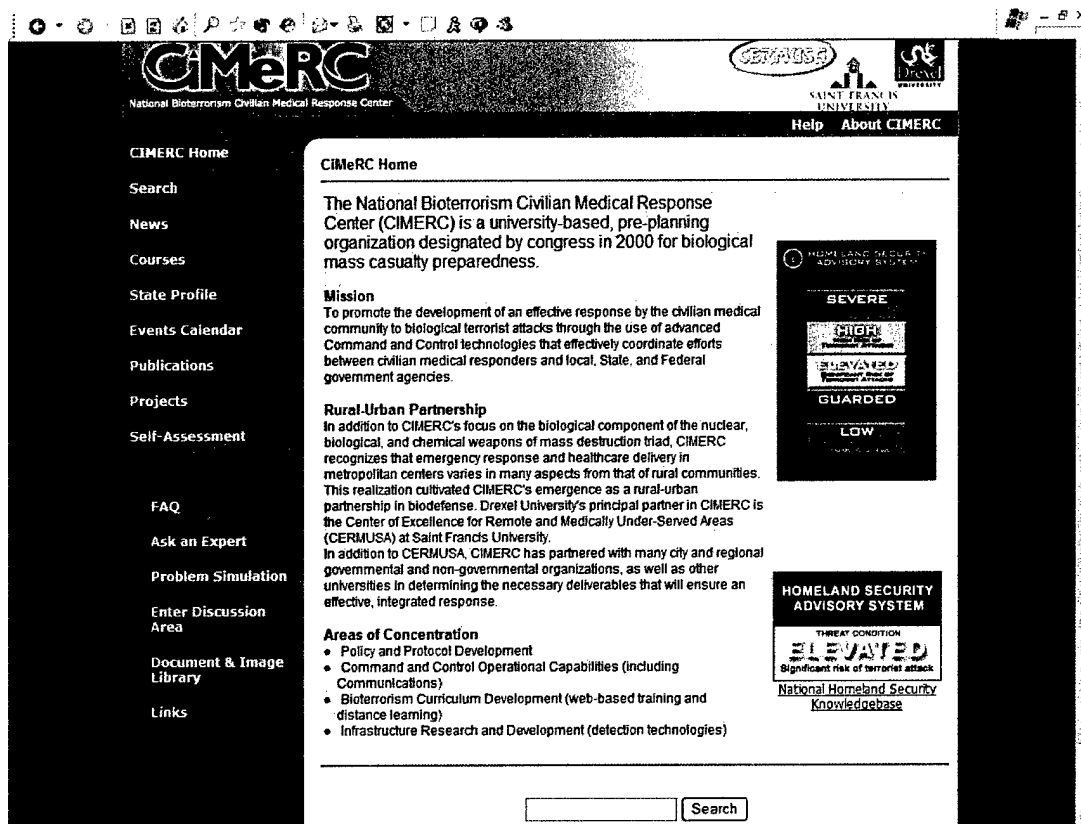
The elements of the template's menu bar are FAQs, Ask An Expert service, Problem Simulation service, Discussions, and Resources. A State Profile section was added to the existing CIMERC functionality. The following pages provide descriptions and illustrations of the Forum's major functional areas.

FAQ's provide a highlighted section of previous answers and responses, pre-selected and organized to facilitate ease of use. Users pursue the information seeking process in an interactive environment and often site designers and community leaders cannot anticipate the user's pathways to knowledge, particularly given our current state of user study. As an illustration, let us follow the question-asking answer-seeking process on the Forum as a linear one, with the first step being that of browsing frequently asked questions, followed by searching archives of previous question and answer exchanges, and finally culminating in posing a query to an expert.

Figure 2: the FAQ page

FAQs

What is the Education Forum?

What is required to access the CIMERC site?

I have a question on bioterrorism, where do I go?

Where can I submit a plan of action for bioterrorism scenarios?

I am part of emergency response team. Where can I receive feedback on my level of preparedness?

I am trying to find documents, images and links related to bioterrorism

Can I make postings for community review and response?

Where can I view upcoming events?

Where can I read news related to bioterrorism?

I live in _____. What specialized resources exist for me?

I am looking for information on _____

How can I contact CIMERC?

I've read the FAQs and I still have a question

What is the Education Forum?

The Education Forum is the interactive, community building section of the CIMERC site. Discussions, problem scenarios and electronic resources are available.

Navigation menu: CIMERC Home, Search, News, Courses, State Profile, Events Calendar, Publications, Projects, Self-Assessment, FAQ, Ask an Expert, Problem Simulation, Enter Discussion Area, Document & Image Library, Links

Help   About CIMERC

For example, if a user has a question about integrating local law enforcement into a Strategic National Stockpile receipt, storage and dissemination plan, this user may attempt to find relevant information on a FAQ page that has been carefully edited and organized with starting points to expedite a user's search for an answer. Failing that, in our linear illustration the user may search the Ask–An-Expert archives. The user may browse the archive by thread or may search, by keyword, through the entire archive for individual messages.

The question above should be reflected on the screen shot.

Figure 3: The Ask An Expert archive screen
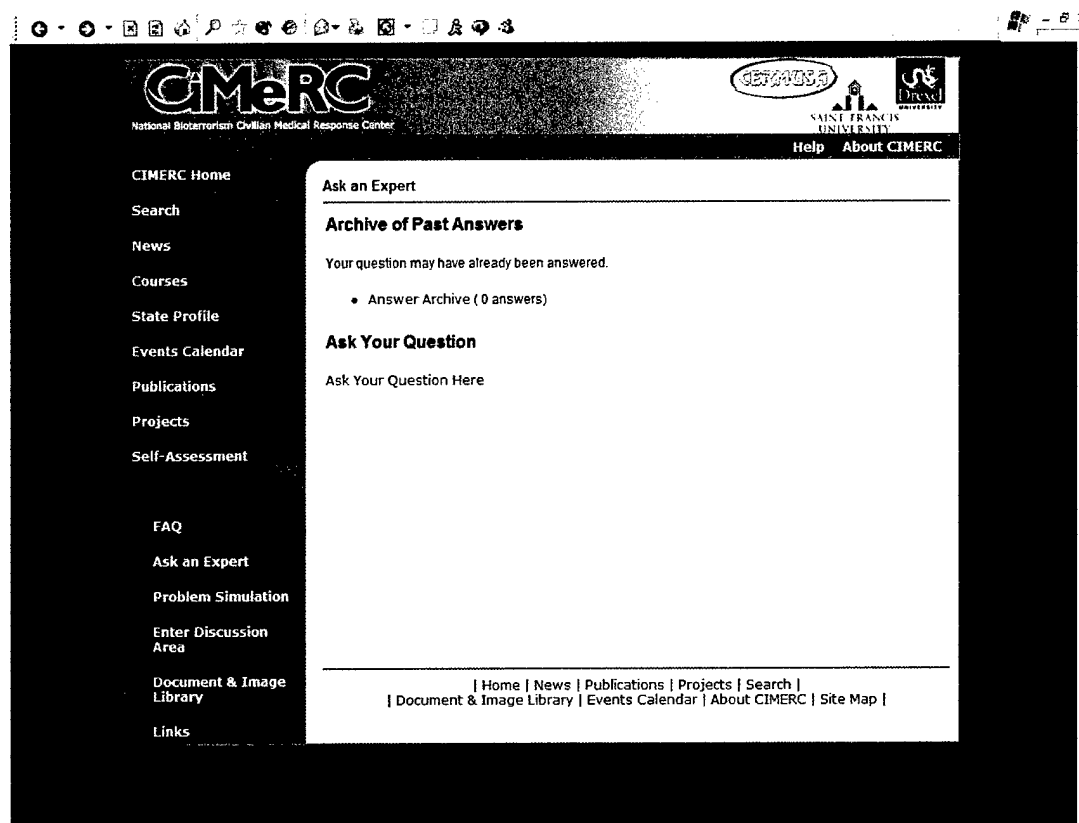
The final step in the expert query process is actually to ask a question of an Expert. To follow the example presented in the previous few screens the question posed may be, "What suggestions do you have about integrating local law enforcement into a Strategic National Stockpile receipt, storage and dissemination plan? The screen follows:

Figure 3: The Ask An Expert Question Screen

Once a user has asked his or her question, an identified expert reviews the question and responds. The conversation is a private one. If the expert thinks that the interaction is one that is worthy of public use, the expert will publish the question (with the permission of the questioner). There is a limit to the knowledge building aspect of the site, inherent in this process. Only exemplary materials will be publicly available. While the most erudite conversations may be cataloged as special archives, the ordinary interactions are not being recorded in the public knowledge domain. This is a policy decision that may be re-examined upon expert and user satisfaction. A sample of an Ask An Expert Office screen is below:

Discussion office pages are similar in design to Ask An Expert. Rather than the private query and response process between user and expert or between expert and expert, the discussion areas promote public conversations among users.

Problem Simulations may be created and posted as the answer form part of a page template. – this section is unclear, please clarify The Tularemia Outbreak Exercise in the screen below is one such example. An answer and response process will then connect users with experts. The expert will respond to the user's answers to the problem situation and then guide and mentor that user. No publishing of private discussions is currently planned, but it would add to the knowledge base being built on the site and the software is readily adapted. This is another policy decision that will need to be re-examined upon use of the site. A sample of a problem simulation screen follows (the office is similar to the Ask An Expert office):

The Document and Image Library has several ways to retrieve resources, through text search, through metadata search, or through browsing a web master/administrator generated browse structure. In addition, there is full text search of the entire site. A sample of the front page to the Document and Image Library is shown below:

A sample of a Document and Image Library search page:

The Document and Image Library office allows the administrator to enter three types of resources, text resources, images, or internet resources (URLs). The administrator may build her or his browse structure dynamically. The Document and Image Library office is a client rather than a server application.

Community Status

Civilian medical emergency response subject matter experts (SMEs) attended a combination of four official meetings, and other group and individual community building opportunities were held to solicit their input and feedback, which provided necessary elements to modify the content and display of the Biodefense Education Forum. CIMERC staff identified SMEs through previous CIMERC interactions and categorized the experts by their area of practice: urban or rural.

Drexel University hosted the first meeting in Philadelphia, Pennsylvania. CIMERC staff identified SMEs attending this meeting as experts in urban biodefense focus specialities, e.g., EMS management. The meeting facilitator focused on educating SMEs about the opportunities involved with the Biodefense Education Forum and on soliciting their feedback about how it could benefit their type of work.

Through focus group interactions, invited experts raised several issues that were discussed and deliberated. Four major outcomes emerged from the initial SME meeting: 1) add a public component to the site, 2) clarify the difference between mentor, expert and participant as they relate to the Biodefense Education Forum, 3) specify security requirements for private portions of the Biodefense Education Forum, 4) provide an organized selection of biodefense resources for the civilian medical response community.

Similarly, the rural subject matter expert meeting utilized a focus group methodology for data collection. The group recognized three critical needs in this meeting: 1) create a network of resources and people (infrastructure) through the Biodefense Education Forum, 2) clarify the rural expert's role in the virtual biodefense community, and 3) provide a mechanism for sharing so that monies earmarked for rural development may be more efficiently leveraged. Most attendees participated on site at Saint Francis University in Loretto, Pennsylvania. However, a number of participants from Wisconsin and other parts of Pennsylvania interacted through a distance learning mechanism, which integrated video and audio elements delivered through the Internet.

The final two group meetings integrated experts from the rural and urban areas to discuss next steps for the Biodefense Education Forum. Participants joined discussions held at Saint Francis University as well as Drexel University and interacted through the Biodefense Education Forum discussion group. The following items emerged as pressing issues to be addressed during the next few months.
1)   Offer continuing education units for completing CIMERC educational components
2)   Establish higher-level security for confidential components of the website
3)   Populate database with useable and useful web-based tools

Discussion and Conclusions

The first phase of the project has focused on the development of the Forum for the Civilian Medical Emergency Response Community. The portal software design and hardware architecture accommodates multiple biodefense response communities and provides a unique learning environment for the advancement of a virtual Civilian Medical Emergency Response Community. Additionally, CIMERC will extend this concept to other first responder communities (e.g., transportation and public health). The transportation sector, with its emphasis on emergency response logistics and physical security, and the public health sector, with its holistic systems perspective, are logical additions to the existing emergency medical community.

The community will be built through continual evaluation and assessment to determine whether the users are making the appropriate connections with one another and with the content they seek. Face-to-face workshops, focus groups, surveys and a webmaster function are essential evaluation process elements. This process will support early adopters who want to perform a function such as develop and discuss case studies or to volunteer to answer questions. The concentration of year II efforts center on community building, evaluation, and addressing feedback to build interaction and to create a dynamic knowledge base from those interactions.

The functionality and services that are available in the Forum will be extended and deepened in reaction to feedback from expert and user groups. The key development process, having created a site with a range of essential functions, is to study user activity and work with emergent lead participants to identify the most critical needs and the new features that would most encourage and leverage their participation. Segmentation of data, data access, and presentation as well as user tracking will be a focus of the software development in Phase II. Login and registration software may well be a strong element in achieving these goals and it has been architected into the original design. The policy decision of best community building practices remains and will need to be addressed before future development is initiated.

In conclusion the iterative process of Civilian Medical Emergency Response Community interaction, measuring and reacting to that interaction, using lessons learned to build complementary communities and to integrate the disparate communities into a single whole, and providing the online environment for those activities is the essence of projected developments for future work.

APPENDIX F1

WORKS CITED

Bonk, C. J., & Wisher, R. A. (2000). Applying collaborative and e-learning tools to military distance learning: A research framework. (Technical Report #1107). Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, Retrieved January 22, 2004 from http://www.publicationshare.com/docs/Dist.Learn(Wisher).pdf

Renninger, K. A., and Shumar, W. (in press). Learning at and with The Math Forum. In S. Barab, R. Kling, & J. Gray (Eds.), *Designing for virtual communities in the service of learning.* New York, NY: Cambridge University Press.

Renninger, K.A. & Shumar, W. (2002). Community building with and for teachers: *The Math Forum* as a resource for teacher professional development. In K.A. Renninger & W. Shumar (Eds.), *Building virtual communities: Learning and change in cyberspace.* New York, NY: Cambridge University Press.

Shumar, Wesley and Renninger, K. Ann Sustaining Online Community: Learning and Participation at The Math Forum, paper presented at the American Educational Research Associaton annual meeting, April 3, 2002, New Orleans, LA.

ScientificAmerican.com editors, 2002 Sci/Tech Web Awards: Mathematics (2002, June 3), Retrieved December 9, 2003 from http://www.scientificamerican.com/article.cfm?articleID=0002B589-9814-1CFB-93F6809EC5880000

ADDITIONAL RESOURCES

Barab, S. A., & Duffy, T. M. (2000). From practice fields to communities of practice. In D. Jonassen & S. Land (Eds.), Theoretical Foundations of Learning Environments (pp. 25-56). Mahwah, NJ: Lawrence Erlbaum Associates.

Bransford, J. S., Brown, A. L., & Cocking, R.R. (1999). How people learn: Brain, mind, experience, and school. Washington, D.C.: National Academy Press.

Brown, J.S., Collins, A., & Duguid, P., (1989). Situated cognition and the culture of learning. *Educational Researcher* 18, 32-42.

Brydon-Miller, M. (1997). Participatory action research: Psychology and social change. *Journal of Social Issues, 53*(4), 657-666.

Chaiklin, S. & Lave, J. (Eds.) (1993). Understanding practice: Perspectives on activity and context. New York, NY: Cambridge University Press.

Cole, M., Engestrom, Y., Vasquez, O. (Eds.) (1997). *Mind, culture and activity: Seminal papers from the Laboratory of Comparative Human Cognition.* New York, NY: Cambridge University Press.

Crowley, K. & Schunn, C.D. (Eds.) (2001). *Designing for science: Implications from everyday, classroom, and professional settings* (pp. 141-173). Mahwah, NJ: Lawrence Erlbaum Associates.

Dey, I. (1999) Grounding grounded theory: Guidelines for qualitative inquiry. San Diego: Academic Press.

Glaser, B. G. (1992). Basics of grounded theory analysis: Emergence vs forcing. Mill Valley, CA: Sociology Press.

Hogen, K. & Pressley, M. (Eds.) (1997). Scaffolding student learning: Instructional approaches and issues. Cambridge, MA: Brookline Books.

Kirshner, D. & Whitson, J. A., (1997). Situated cognition: Social, semiotic and psychological perspectives. Mahwah, NJ: Lawrence Erlbaum and Associates.

Lave, J., & Wenger, E. (1991). Situated learning : Legitimate peripheral participation. New York: Cambridge University Press.

Linehan, C. & McCarthy, J. (2000). Positioning in practice: Understanding participation in the social world. Journal for the Theory of Social Behavior 30(4).

Marcus, H., & Nurius, P. (1986). Possible selves. American Psychologist, 4(9), 954-969.

Mitchell, I. (1992). Sustaining support and stimulation: The Teacher Group 1986-9. In J.r. Baird & J. R. Northfield, Learning from the PEEL experience. Melbourne, Victoria: Monash University Printing Services.

Renninger, K. A. & Boone, S. (September, 2001). The Math Forum's Bridging Research and Practice Project: A Collaboration to encourage mathematical thinking. NCTM Conference on Practitioner Research in Mathematics Education. Albuquerque, New Mexico.

Renninger, K. A. & Farra, L. (2003). Mentor-participant exchange in the Ask Dr. Math service: Design and implementation considerations. In M. Mardis (Ed.), Digital Libraries as Complement to K-12 Teaching and Learning. ERIC Monograph Series.

Renninger, K. A. & Hidi, S. (2002). Student interest and achievement: Developmental issues raised by a case study. In A. Wigfield & J. S. Eccles (Eds.), Development of achievement motivation (pp. 173-195). San Diego, CA: Academic Press.

Renninger, K. A. & Shumar, W. (April, 2003). The role of the social in teachers' interest development and learning with an online community. Paper presented as part of the symposium, Sociocultural Aspects of Interest Development and Their Implications for Education (S. Nolen, Chair). American Educational Research Association, Chicago, IL.

Renninger, K. A. (2000). Individual Interest and Its Implications for Understanding Intrinsic Motivation. In C. Sansone & J. M. Harackiewicz (Eds.), Intrinsic and extrinsic motivation: The search for optimal motivation and performance (pp. 375-404). New York: Academic.

Renninger, K. A., Farra, L., & Feldman-Riordan, C. (2000). The impact of The Math Forum's Problems of the Week on students' mathematical thinking. Proceedings of ICLS 2000. Mahwah, NJ: Lawrence Erlbaum Associates (www.mathforum.org/articles/rennin2_2000.html)

Renninger, K.A. & Shumar, W. (April, 2001). Multidimensional aspects of on-line community building: The Math Forum. Paper presented as part of the symposium, Understanding online learning communities: Sociocultural views. American Educational Research Association. Seattle, WA.

Renninger, K.A., Weimar, S.A. & Klotz, E.A. (1998). Teachers and students investigating and communicating about geometry: The Math Forum. In R. Lehrer & D. Chazan (Eds.) Designing learning environments for developing understanding of geometry and space(pp. 465-487). Mahwah, NJ: Lawrence Erlbaum Associates.

Rogoff, B. (1995). Observing sociocultural activity on three planes: Participatory appropriation, guided participation, and apprenticeship. In J.V. Wertsch, P. del Rio, & A. Alvarez (Eds.), Sociocultural studies of mind (pp. 139-164). Cambridge, England: Cambridge University Press.

Rogoff, B. (1998). Cognition as a collaborative process. In D. Kuhn & R. S. Siegler (Vol. Eds.) Cognition, perception, and language (vol. 2), in W. Damon (Gen. Ed.), Handbook of child psychology (5th ed., pp. 679-744). New York: John Wiley and Sons.

Schauble, L. & Glaser, R. (1990). Scientific thinking in children and adults. Contributions to Human Development, 21, 9-27.

Shulman, L.S, (1986). Those who understand: Knowledge growth in teaching. Educational Researcher, 15, 4-14.

Shumar, W. & Renninger, K. A. (in press)

Shumar, W. (2003) The role of community and belonging in online learning. To appear in M. Mardis (Ed.) Developing Digital Libraries for K-12 Education. ERIC Monograph Series.

Siegler, R.S. (1996). Emerging minds: The process of change in children's thinking. New York: Oxford University Press.

Strauss, A., & Corbin, J. (Eds.). (1997) Grounded theory in practice. Thousand Oaks, Ca.: Sage.

Tweney, R.D. (2001). Scientific thinking: A cognitive-historical approach. In K. Crowley & C.D.Schunn (Eds.), Designing for science: Implications from everyday, classroom, and professional settings (pp. 141-173). Mahwah, NJ: Lawrence Erlbaum Associates.

Wertsch, J.V. & Toma, C. (1995). Discourse and learning in the classroom: A sociocultural approach. In L. P. Steffe & J. Gale (Eds.), Consructivism in education. Hillsdale, NJ: Lawrence Erlbaum Associates.

Building the Application Server

- Purpose Statement
- Intended Audience
- Note
- Adjustments
- Operating System
- Build Procedure And Detailed Configuration
  - o List of Packages needed
  - o Perl Modules Installed
  - o Building
  - o Mod_Perl
  - o Apache
  - o Mason
  - o Glimpse
  - o Other
- Author

Purpose Statement

Installation guide for application server

```
Apache and perl are seamlessly glued together by the `mod_perl' server
plugin, making it is possible to write Apache modules entirely in Perl.
In addition, the persistent interpreter embedded in the server avoids
the overhead of starting an external interpreter and the penalty of Perl
start-up time.

--perl.apache.org
```

This file is a general reference to build an application server running apache, mod_perl, perl, mason.

Intended Audience

This is the file to aid a Red Hat Linux system administrator to set up or install a similar application server.

Note

There will be resources noted throughout the document that one will have to reference while using this document to set up apache with mod_perl application server or troubleshoot any problems during the installation.

USAMRMC Log No.: 02101001

You will see a message on the screen:

```
"This system is currently configured for Microsoft Windows 2000/Windows
.NET"
```

By pressing F9 key you can change this message.

Choose:

```
"System Options" --> "OS selection"

highlight "linux" instead of "Microsoft Windows 2000/Windows .NET"
```

Operating System

Install Red Hat Enterprise Linux Version 2.1 with RAID1

Build Procedure And Detailed Configuration

This outlines all the needed packages, modules, build procedure, and configuration scripts responsible for setting up the application server.

List of Packages needed

```
Perl (You got it when installing OS)
apache_1.3.28.tar.gz
  - http://archive.apache.org/dist/httpd/
mod_perl-1.28.tar.gz
  - http://perl.apache.org/download/index.html
HTML-Mason-1.22.tar.gz
  - http://www.masonhq.com/code/download/
glimpse-latest.tar.gz
  - http://webglimpse.org/
sqsh-2.1-linux-12.5.tar.gz
  - http://www.sqsh.org/
sybase-common-12.5.0.1SBE-1.i386.rpm
sybase-esql-12.5.0.1ESD-1.i386.rpm
sybase-openclient-12.5.0.1ESD-1.i386.rpm
```

Perl Modules Installed

CPAN Introduction: CPAN is the Comprehensive Perl Archive Network, a large collection of Perl software and documentation. Please refer to http://www.cpan.org/misc/cpan-faq.html for more information.

1. From CPAN:

    Apache-AuthCookie-3.04
    DBI-1.38
    MD5-2.02
    Apache-Test-1.04
    Devel-StackTrace-1.04
    Net-Daemon-0.37
    Archive-Tar-1.05
    Devel-Symdump-2.03
    Net-Telnet-3.03
    Attribute-Handlers-0.78
    Digest-MD5-2.27
    Params-Validate-0.65
    Bundle-libnet-1.00
    Digest-SHA1-2.04
    PlRPC-0.2017
    Cache-Cache-1.02
    Error-0.15
    Scalar-List-Utils-1.13
    Class-Container-0.10
    Exception-Class-1.16
    Storable-2.08
    Class-Data-Inheritable-0.02
    File-Spec-0.86
    TermReadKey-2.21
    Compress-Zlib-1.22
    HTML-Mason-1.23
    Term-ReadLine-Perl-1.0203
    CPAN-1.76
    IO-Tee-0.64
    Test-Harness-2.30
    Data-Dumper-2.121
    libapreq-1.3
    Test-Simple-0.47
    DBD-Multiplex-1.9
    libnet-1.17
    Text-Reform-1.11
    DBD-Sybase-1.01
    Mail-Sender-0.8.08
    Time-HiRes-1.51
    Time-Piece-1.08
    libwww-perl-5.69
    CPAN.pm
    libnet.pm

2. From Forum:

    AccessHandler
    AuthCookie
    Log
    Util
    Puzzler
    DB

```
DBhandle
Key
Handler
Glimpse
Error
Search
People
```

Building

The following will build up all of the applications.

Download all the tarballs We'll assume that all the sources go to:

```
/usr/local/src/archive dir.
```

First let's make archive directory:

```
mkdir /usr/local/src/archive

cd /usr/local/src/archive
```

Download all the tarballs mentioned in the package list above here.

Get the server source ready, extract the distributions

```
cd /usr/local/src/

tar -xvzf archive/apache_1.3.28.tar.gz

tar -xvzf archive/mod_perl-1.28.tar.gz

...
```

Create links for all the files, this will make life easier later on.

```
ln -s apache_1.3.28 apache

ln -s mod_perl-1.28 mod_perl
```

Mod_Perl

Caution: Mod_perl cannot work as DSO with Apache well. If you do so, Apache will be unstable.

Compile mod_perl statically into Apache

Set the default target directory of the apache installation.

```
cd apache

./configure --prefix=/usr/local/httpd
```

Install the Perl side of mod_perl into the Perl hierarchy and prepare the src/modules/perl/ subdirectory inside the Apache source tree:

```
cd ../mod_perl

perl Makefile.PL \

        EVERYTHING=1 \

        APACHE_SRC==../apache_1.3.28/src \

        USER_APACI=1 \

        PREP_HTTPD=1 \

        DO_HTTPD=1 \

        DYNAMIC=1

make

make test

make install
```

The APACHE_SRC option sets the path to your Apache source tree.

The USE_APACI option triggers the new hybrid build environment

The PREP_HTTPD option forces preparation of the APACHE_SRC/modules/perl/ tree but no automatic build.

Apache

Keep DSO support in Apache. This allows you to load other things (needed modules).

```
cd ../apache

./configure \

        --prefix=/usr/local/apache \

        --sysconfdir=/etc/httpd \
```

```
--logfiledir=/var/log/httpd \

--cgidir=/var/www/cgi-bin \

--enable-module=rewrite \

--enable-shared=rewrite \

--enable-module=so \

--activate-module=src/modules/perl/libperl.a \

--disable-shared=perl \

--enable-module=perl

--...
```

(Add other appropriate switches. Due to the version difference, the switches are needed to be adjusted. Reference the file on /usr/local/src/make/make-apache)

```
make

make install
```

Test to see whether everything went well:

```
httpd -l

OUTPUT:

    Compiled-in modules:
        http_core.c
        mod_so.c
        mod_perl.c
```

Check for this line in /etc/httpd/conf/httpd.conf:

```
AddModule mod_perl.c
```

Mason

Mason Installation: at this stage, Perl, Apache and mod_perl are already installed.

Mason allows web pages and sites to be constructed from shared, reusable building blocks called components. Components contain a mix of Perl and HTML, and can call each other and pass values back and forth like subroutines. Components increase modularity and eliminate repetitive work

Please refer to the following URL for general documentation, FAQ, mailing lists, and troubleshoot needs.

http://www.masonhq.com

Prerequisites

Mason requires Perl 5.005 or greater, and the following CPAN modules:

```
Params::Validate
Exception::Class
Class::Container
File::Spec
Scalar::Util
```

The following CPAN modules are optional:

```
Apache::Request
Cache::Cache
CGI.pm
```

Installation

```
cd /usr/local/src
cd HTML-Mason-0.89
perl Makefile.PL
make
make install
```

Configure /etc/httpd/conf/httpd.conf for Mason

```
cd /etc/httpd/conf/
vi httpd.conf
```

Add the following lines to httpd.conf:

```
PerlRequire    conf/handler.pl

<Location />
   SetHandler  perl-script
   PerlHandler HTML::Mason
</Location>
```

Edit above bracket to refer to /etc/httpd/conf/httpd.conf later on.

Now create the file handler.pl (/etc/httpd/conf/handler.pl):

```
cd /etc/httpd/conf/
vi handler.pl
```

Refer to /etc/httpd/conf/handler.conf on application server

Restart Apache

```
/usr/local/apache/bin/apachectl restart
```

Test

Now you can write a test file (/var/www/html/test.html):

```
<HTML>
 <HEAD>
  <TITLE>Mason Test</TITLE>
 </HEAD>
 <BODY BGCOLOR="#FFFFFF">
  <H1>Mason Test</H1>
%  my $noun = 'World';
  Hello <% $noun %>!
 </BODY>
</HTML>
```

Go to your browser: http://hostname/test.html. You should see 'Hello World!'

Glimpse

Glimpse is a text indexing and searching system

```
sh configure
make
make install
```

Modify /etc/httpd/conf/httpd.conf:

Open /etc/httpd/conf/httpd.conf and add following lines as global Glimpse variables setting:

```
# global Forum-Glimpse variables
PerlSetEnv GLIMPSE_INDEX_PATH "/var/www/search/indexes"
PerlSetEnv GLIMPSE_FILES_PATH "/var/www/search/files"
PerlSetEnv GLIMPSEBIN "/usr/bin/glimpse"
PerlSetEnv SEARCHCTRL "/var/www/search/ctrl"
```

The WWW home page for glimpse is in http://glimpse.cs.arizona.edu/ It includes links to the source, binaries for most UNIX systems, documentations, articles, and more.

Other

Install Sybase client site and sqsh per its documentation.

Author

Jessica Zhu, jessica@mathforum.org

Building the Application Server

Installation Notes on the Application Servers

- Description
- htaccess: (biodefense/html)
- MakeFile: (biodefense/html)
- handler.pl: (/etc/httpd/conf)

Description

Installation & Configuration Notes for BioApp

This document contains notes on changes made during installation between mathforum's testapp server and biodefense's bioapp server.

---

htaccess: (biodefense/html)

1) Contains environment variables for database interaction:

```
Server
User
Password
Database
```

These values are filled in with appropriate values determined by the Makefile. This is necessary because the certain values are different Server Name (biodb instead of SYBASE), and passwords.

MakeFile: (biodefense/html)

1) Includes bio option.

2) To change to a new domain name set BIO_APP_URI eg:

```
BIO_APP_URI=http://proapp.old.mathforum.org/$(RELEASE_SHORT)
```

---

handler.pl: (/etc/httpd/conf)

1) Added parameter to ApacheHandler instantiation to force POST and GET arguments to use CGI.pm (args_method => 'CGI') This appears to have been the default in previous versions (ie that of testapp) and had been changed.

http://www.masonhq.com/docs/manual/ApacheHandler.html

2) this handler differs from testapp in that there is no CPU logging. Image and .js handling were brought over to the current script.

Installation Notes on the Application Servers

Database Server

- Description
- Adjustments
- Build Procedure And Detailed Configuration
- Partition Table
- Operating System
- Package List For Building
- Build Procedure
  - o Install Sybase
- Author

Description

Installation guide for database server

Adjustments

You will see the message on the screen: ``This system currently configured for Microsoft Windows 2000/Windows .NET"

By pressing F9 key you can change this message.

Choose:
  ``System Options" --> ``OS selection"
  highlight ``linux" instead of ``Microsoft Windows 2000/ Windows .NET"

Build Procedure And Detailed Configuration

This outlines the partition table layout, needed rpm files, the build procedure and configuration scripts responsible for the application server setup.

Partition Table

Configure and build raid1 when installing the OS. Here is the general layout for partiotion table.

```
/               1G
/boot           150M
/dbdata         44G
/dbtrans        14G
/usr            11G
/var            500M
```

Red Hat Enterprise Linux Version 2.1

Package List For Building

```
sybase-doc-12.5.0.1ESD-1.i386.rpm
sqsh-2.1-linux-12.5.tar.gz
sybase-efts-12.5.0.1ESD-1.i386.rpm
sybase-ase-12.5.0.1ESD-1.i386.rpm
sybase-esql-12.5.0.1ESD-1.i386.rpm
sybase-common-12.5.0.1SBE-1.i386.rpm
sybase-openclient-12.5.0.1ESD-1.i386.rpm
```

Build Procedure

Load Linux according to the partition layout with RAID1. Also make a boot disk.

Install Sybase

Adjust shared memory kernel value for sybase The OS shared memory default for most Linux release is 32MB. The minimum required by Sybase Adaptive server is 64MB. So the maximum shared memory segment size is needed to be tuned. This can be done by typing:

```
echo 67108864 > /proc/sys/kernel/shmmax
```

```
  This helps dynamically tune the Linux kernel.  Its effects will be gone
when the system gets rebooted. So add this line in /etc/rc.d/rc.local
  to avoid having to type this command every time when the box gets rebooted.

If you have enough memory, you can echo more memory to shmmax.
```

Create sybase group and user

```
su
groupadd sybase
useradd -g sybase -d /home/sybase -c "Sybase ASE DBA account" -p ???
sybase
```

Insert the Sybase CD, install all sybase rpm files

```
rpm -Uvh sybase-common-12.5.0.1SBE-1.i386.rpm
rpm -Uvh sybase-ase-12.5.0.1ESD-1.i386.rpm
rpm -Uvh sybase-doc-12.5.0.1ESD-1.i386.rpm
rpm -Uvh sybase-esql-12.5.0.1ESD-1.i386.rpm
rpm -Uvh sybase-efts-12.5.0.1ESD-1.i386.rpm
rpm -Uvh sybase-openclient-12.5.0.1ESD-1.i386.rpm
```

● Configure sybase

```
su - sybase
./startd.sh $SYBASE/$SYBASE_SYSAM
lmgr
```

Enter all the information about Sybase License Certificate

Make sure sybase license is successfully installed.

Check the license status by entering:

```
$SYBASE?SYSAM?bin/lmutil lmstat -c
```

Configure sybase

```
asecfg
```

Follow all the screen do the configuration and refer to the parameters adjustment made on biodb server.

●
```
The main values adjusted as follows:
ASE page size(kb): 4 KB
Master device size(MB): 300
Master database size(MB):24
Sybsystemprocs device size(MB): 300
Sybsystemprocs database size(MB):120
```

```
Test sybase configuration

  isql -Usa -SServer_Name
```

enter the password

```
> select @@ version
> go
```

Set up password for sa

```
> exec sp_password NULL, "password"
> go
```

Add a new login name with sp_addlogin

●

```
> exec sp_addlogin "sybtest", "password"
> go
```

Author

Jessica ZHU jessica@mathforum.org

Database Server

Application Setup: Log Files

- Description
- Log Files
- Creating Log Files

Description

After installing the database and Forum::People module, log files must be manually created to allow signup notification in discussions and e-mail notification.

Log Files

The people database (see Sybase : Schemas : People) and the perl module that use it (Forum::People) log every time somebody subscribes for notification, unsubscribes from notification, and every time a notification message is sent. These log files are in the directory /var/log/subscriptions .

Creating Log Files

Create the directory /var/log/subscriptions and, in it, the log files ``notify_log'' and ``subscribe_log''. These files must be made writable to the web server (group writable, group ``nobody'').

Application Setup: Log Files

Security Setup

- Description
- Packet Filtering Firewall
- DoS Protection
- Password File Definition
- Services
- Tripwire
- Author

Description

Security setup for servers

Packet Filtering Firewall

Packet filtering firewall is set up on the bio machines. Basically, the firewall will open smtp(sendmail), http(apache), ssh, dns(domain), and sybase ports on the application server and open ssh, dns, sybase ports on the database server, accept all local traffic, and rejecting all other input.

The file is /etc/sysconfig/ipchains. Edit when necessary.

DoS Protection

```
a. Source route verification enabled
b. Reply to ICMP echo requests on broadcast and multicast address prevented
c. Log datagram suspected to be spoofed IP address
d. Prevent from ping to death
```

Please refer to /etc/sysctl.conf

Password File Definition

Password checking:

```
length
lifetime
dictionary check
```

Please refer to /etc/login.defs

Services

Turn off all unnecessary services in the system.

```
/sbin/chkconfig --list
```

Tripwire

Setup tripwire on both bio machines.

Author

Jessica Zhu jessica@mathforum.org

Security Setup

Data Initialization

- Description
- Setup
- Get Device Info
- Create Devices
- Select Database Information
- Create New Databases
    - discussions
    - people
    - biodefense
- User Account
    - Add a new user account, password, default database
    - Add a user to existing databases
- Backup
- Author

Description

Initializing Sybase databases

The following are SQL statements or Sybase configuration commands entered through sqsh. To begin, login as sa to Sybase using sqsh.

Setup

This is **very useful** to add to your .sqshrc file -- saves you from typing 'go' about a million times.

```
\set semicolon_hack=1
```

The following is a **one-time** Sybase configuration change (the default is 10 devices):

```
use master;
sp_configure "number of devices", 20;
```

Get Device Info

This tells about existing data devices -- useful for deciding if you need to add some devices before expanding or creating new databases.

```
SELECT     low/16777216 AS vdevno,
           CONVERT (VARCHAR(60), phyname) AS phyname
```

```
FROM      sysdevices
ORDER BY  low;
```

Create Devices

Create 6 new data devices and 6 transaction log devices -- plenty for now. Each of these commands takes a few minutes.

```
   disk init name='dbdata2', physname='/dbdata/dbdata2.dat', vdevno=2,
size=1048575;
   ...
   disk init name='dbdata7', physname='/dbdata/dbdata7.dat', vdevno=7,
size=1048575;

   disk init name='dbtrans8', physname='/dbtrans/dbtrans8.dat', vdevno=8,
size=524287;
   ...
   disk init name='dbtrans13', physname='/dbtrans/dbtrans13.dat', vdevno=13,
size=524287;
```

Select Database Information

This tells about existing databases and how full they are -- useful for determining when to expand an existing database.

Note: sizes are reported in 4-k blocks

```
SELECT    CONVERT (VARCHAR(10), su.dbid)               AS 'dbid',
          CONVERT (VARCHAR(20), sd.name)               AS 'database name',
          CONVERT (VARCHAR(10), su.segmap)             AS 'segmap',
          CONVERT (VARCHAR(20), sv.name)               AS 'device name',
          CONVERT (VARCHAR(10), su.size/256)           AS 'size MB',
          CONVERT (VARCHAR(10), su.unreservedpgs/256) AS 'free MB'
FROM      sysusages su, sysdatabases sd, sysdevices sv
WHERE     su.dbid = sd.dbid
AND       su.vstart >= sv.low
AND       su.vstart < sv.high
ORDER BY  su.dbid, su.segmap;
```

Create New Databases

discussions

the create statement will take a half hour or more

```
use master;

CREATE DATABASE discussions ON dbdata2  = 2000
        LOG                 ON dbtrans8 = 200;
```

```
sp_dboption discussions, 'allow nulls by default', true;
sp_dboption discussions, 'abort tran on log full', true;
```

people

the create statement will take a half hour or more

```
use master;

CREATE DATABASE people ON dbdata3  = 2000
        LOG            ON dbtrans9 = 200;

sp_dboption people, 'allow nulls by default', true;
sp_dboption people, 'abort tran on log full', true;
```

biodefense

the create statement will take a half hour or more

```
use master;

CREATE DATABASE biodefense ON dbdata4   = 2000
        LOG                ON dbtrans10 = 200;

sp_dboption biodefense, 'allow nulls by default', true;
sp_dboption biodefense, 'abort tran on log full', true;
```

User Account

Add a new user account, password, default database

```
use master;
sp_addlogin http, *******, discussions;
```

Add a user to existing databases

```
use discussions;
sp_adduser http;

use people;
sp_adduser http;

use biodefense;
sp_adduser http;
```

Backup

Perform full dump of new databases

```
use discussions;
checkpoint;
use people;
checkpoint;
use biodefense;
checkpoint;
use master;
checkpoint;

use master;
DUMP DATABASE discussions to '/dbdata/discussions_full.txt';
DUMP DATABASE people to '/dbdata/people_full.txt';
DUMP DATABASE biodefense to '/dbdata/biodefense_full.txt';
DUMP DATABASE master to '/dbdata/master_full.txt';
```

Author

David Tristano, davidt@mathforum.org

Data Initialization

Data Backup

- Description
- Database Dumps To File
  - o Cron
  - o Dump script
  - o Files
- Backups
- Author

Description

Dumping and backing up Sybase databases

Database Dumps To File

This outlines the chain of events and files responsible for regular dumps of Sybase databases.

Cron

The dump script is set to run from root's crontab file

```
Read only: [root@biodb root]# cat /var/spool/cron/root
Edit:      [root@biodb root]# crontab -e
```

Dump script

The dump script is located at biodb:/dbdata/backups/all_dump.pl The script is self documented.

Files

The dump script causes Sybase to write out full database dumps once per day to this directory:
/dbdata/backups/full

The dump script causes Sybase to write out transaction log dumps once every 30 minutes to this
directory: /dbdata/backups/tran

Backups

A daily tape backup of the /dbdata partition is recommended.

David Tristano, davidt@mathforum.org

Data Backup

Schemas Overview

- Description
- biodefense database
- discussions database
- people database

Description

The software relies on three databases (besides the usual internal Sybase system data).

---

biodefense database

The biodefense database stores information for the Document and Image Library.

---

discussions database

The discussions database stores information about discussions, including data for the Ask an Expert and Problem Simulation services.

---

people database

The people database stores the e-mail addresses of people who have signed up for e-mail notification.

Schemas Overview

Biodefense

- Description
- Resources table
- Images table
- ExternalLinks table
- Files table

Description

The biodefense database stores information for the Document and Image Library.

Resources table

The resources table is the defining table. It is contains information for all the elements of the document library. Additional meta-data is contained in the other tables (Files, Images, ExternalLinks). The ID field is referenced by the other tables.

```
create table Resources
(
      ID          INTEGER PRIMARY KEY NOT NULL,
      CimercID    VARCHAR(255),
      Style       VARCHAR(255),
      Title       VARCHAR(255),
      Description TEXT,
      Author                   VARCHAR(255),
      AuthorEmail              VARCHAR(255),
      ContentProvider          VARCHAR(255),
      ContentProviderEmail     VARCHAR(255),
      CreationDate             DATETIME,
      Keywords    VARCHAR(255),
      Category1   VARCHAR(255),
      Rank1       INTEGER,
      Category2   VARCHAR(255),
      Rank2       INTEGER,
      Category3   VARCHAR(255),
      Rank3       INTEGER,
      Category4   VARCHAR(255),
      Rank4       INTEGER,
      Category5   VARCHAR(255),
      Rank5       INTEGER
)
```

Images table

This table contains the reference to the Resources table, its own ID as an image and the FileName. The FileName is the location the web link will point to.

```
create table Images
(
    ID          INTEGER PRIMARY KEY NOT NULL,
    ResourceID  INTEGER NOT NULL,
    FileName    VARCHAR(255),
    constraint fk_tbImages_r
        foreign key (ResourceID)
        references Resources (ID)
)
```

ExternalLinks table

This table contains the reference to the Resources table, its own ID as a Link and the URI. The URI is the link.

```
create table ExternalLinks
(
    ID          INTEGER PRIMARY KEY NOT NULL,
    ResourceID  INTEGER NOT NULL,
    URI         VARCHAR(255),
    constraint fk_ExternalLinks_r
        foreign key (ResourceID)
        references Resources (ID)
)
```

Files table

This table contains the reference to the Resources table, its own ID as a Document and the FileName. The FileName is the location the web link will point to.

```
create table Files
(
    ID          INTEGER PRIMARY KEY NOT NULL,
    ResourceID  INTEGER NOT NULL,
    FileName    VARCHAR(255),
    constraint fk_Files_r
        foreign key (ResourceID)
        references Resources (ID)
)
```

Biodefense

Discussions

- Description
- messages table
- headers table
- threading table
- thread_info table
- discussions table
- annotations table
- mentions table

Description

The discussions database stores discussion messages and all their associated data. It coordinates with the people database to manage notification subscriptions.

---

messages table

The messages table stores information about each message. The message_n column is a unique identifier.

```
create table messages
(
        message_n integer not null,
        date datetime not null,
        author varchar(255),
        email varchar(255),
        subject varchar(255),
        texthtml char(4),                /* should be 'not null' but isn't */
        body text,
        mark_i tinyint,                  /* "interesting" flag, value 1 */
        canon_subject varchar(255) not null default "[no subject]",
        user_id integer,                 /* author's user ID, if known */
)
```

---

headers table

This table is unused by the biodefense system. Its purpose is to store additional information for messages which were derived from e-mail messages.

---

threading table

The threading table maintains the structure of replies. If message_n=13 is a reply to message_n=12, then there is an entry in this table with message_n=13 and parent_n=12.

```
create table threading
(
        message_n integer not null,
        parent_n integer not null,
)
```

---

thread_info table

The thread_info table caches computed information for each message so that the information does not have to be recomputed over and over. It summarizes the message's subthread, that is, the message plus its replies plus their replies, etc. The information is computed based on the messages and threading tables.

```
create table thread_info
(
        message_n integer not null,
        total_kids integer not null, /* number of messages in subthread */
        early_date datetime not null,/* earliest date in subthread */
        late_date datetime not null, /* latest date in subthread */
        mark_i integer not null,     /* number of marked messages */
)
```

---

discussions table

The discussions table has an entry for each discussion. Many of the fields are not used in the biodefense system.

```
create table discussions
(
        name varchar(63) not null,
        root_n integer not null,
        human_name varchar(63) not null,
        short_name varchar(31),
        header_file varchar(255),
        footer_file varchar(255),
        email varchar(255),
        owner_email varchar(255),
        notify_email varchar(255),
        notify_template varchar(255),
        root_url varchar(255),
        custom_dir varchar(255),
)
```

---

annotations table

The annotations table is used to attach (key, value) pairs to messages for special purposes. To keep the SQL correct, the key is called ``facet''.

This is an extremely flexible facility. In the biodefense software, it is used for two purposes. (1) An annotation with facet=``notifier'' and value the name of a software routine is attached to discussions for which notification is turned on. By changing the name, notification could be customized. (2) An annotation with facet=``subscrip'' and value a subscription_id (from the people database) is attached to a discussion for each person who is subscribed for notification.

```
create table annotations
(
 message_n integer not null,
 facet char (8) not null,
 value varchar (255) not null,
)
```

mentions table

The mentions table is not used.

Discussions

People

- Description
- people table
- subscriptions table
- groups table
- permissions table

Description

The people database stores information about people who have subscribed to receive e-mail notification of discussion posts. In principle, the people database supports registration and login with permissions assigned per-user, and notification of any type of event. But supporting software and the user interface to implement these fancy features are not written.

---

people table

The people table stores everything we know about a person. So far, in the biodefense system, only the people_id and email fields are used. The others are always NULL. The other fields would be filled in only for a person who registered.

```
create table people
(
        people_id integer not null,
        /* Users give email and password to log in. */
        email varchar(255),
        password char(16),                /* encrypted */
        last_name varchar(255) not null,
        rest_of_name varchar(255),
        street varchar(255),
        city varchar(255),
        state varchar(31),
        country varchar(31),
        zip varchar(15),                  /* or other postal code */
        phone varchar(15),
        ed_role varchar(7),               /* student, faculty, other */
        url varchar(255),
        organization varchar(63),
        organization_url varchar(255),
        organization_address1 varchar(255),
        organization_address2 varchar(255),
        organization_email varchar(255),
        department varchar(63),
        department_url varchar(255),
        /* The session key is 0 when the user is logged out. */
        session_key int default(0) not null,     /* changed per session */
        session_ip varchar(15),                   /* IP address */
```

```
        last_login datetime,
        create_date datetime not null,
        change_date datetime not null,
        /* Flags, value 0 or 1. NULL means "not relevant here". */
        keep_in_touch tinyint default(0) not null, /* send newsletters, etc.
*/
        registered tinyint,                         /* 0 for authors, etc. */
        public_email tinyint,                       /* public/private */
        public_address tinyint,
        public_phone tinyint,
        public_url tinyint,
        public_organization tinyint,
        public_department tinyint,
)
```

subscriptions table

The subscriptions table maps subscription_id (as stored in the discussions database) to people_id (as stored in this database). The service is always 'Nonpareil', the discussions system, because only discussion notification is provided currently.

```
create table subscriptions
(
        subscription_id integer not null,
        service varchar(15) not null,
        people_id integer not null,
        create_date datetime not null,
        change_date datetime not null,
)
```

groups table

The groups table lists the names of permission groups. It is unused in the biodefense system.

```
create table groups
(
        group_id integer not null,
        group_name varchar(32) not null,
        create_date datetime not null,
        change_date datetime not null,
)
```

permissions table

The permissions table lists the people who are in each permission group, if any. It is unused in the biodefense system.

```
create table permissions
(
        people_id integer not null,
```

```
        group_id integer not null,
        create_date datetime not null,         /* can't be changed */
)
```

People

Password Protecting Directories

- Description
- Condensed:
    - o   Create Password File
    - o   Add a User
    - o   Change a User's Password
    - o   Delete a User
    - o   Create Groups
    - o   Configure Apache
- Apache Docs
- Configuration: Protecting content with basic authentication
    - o   Create a password file
    - o   Set the configuration to use this password file
    - o   Optionally, create a group file

Description

This documentation covers password protecting a directory. There are two sections: Condensed and Adapted Apache Documentation. Condensed lists just the commands and requirements. The second is Apache Documentation adapted for this server.

Condensed:

Create Password File

```
htpasswd -c /usr/local/apache/passwd/passwords user
```

After entering the password for ``user" twice the password is encrypted and the file is created with one user.

Add a User

```
htpasswd /usr/local/apache/passwd/passwords admin
```

Change a User's Password

```
htpasswd /usr/local/apache/passwd/passwords forgot
```

If a user named forgot exists this changes the password. Otherwise it creates a user named forgot with that password.

Delete a User

Delete the line from the passwords file that contains that user's name. Also update the groups file if necessary.

Create Groups

Use a text editor and make the following file:

```
level1: user admin
level2: admin
```

save it as:

```
/usr/local/apache/passwd/groups
```

You have now created the necessary files for Apache to reference. Now apache needs to be told to check these files.

Configure Apache

Create/Append .htaccess file:

The directives are:

```
AuthType Basic
AuthName "Site"
AuthUserFile /usr/local/apache/passwd/passwords
AuthGroupFile /usr/local/apache/passwd/groups
Require group level1
```

If an .htaccess file exists that does not contain Authorization/Authentication directives append the above directives to the .htaccess file.

If an .htaccess file exists that already has Auth* directives then you will need to decide which ones to use.

If no .htaccess file exists then create a file called .htaccess and place it in the desired directory.

Apache Docs

There are two configuration steps which you must complete in order to protect a resource using basic authentication. Or three, depending on what you are trying to do.

```
1. Create a password file
2. Set the configuration to use this password file
3. Optionally, create a group file
```

Create a password file

In order to determine whether a particular username/password combination is valid, the username and password supplied by the user will need to be compared to some authoritative listing of usernames and password. This is the password file, which you will need to create on the server side, and populate with valid users and their passwords.

Because this file contains sensitive information, it should be stored outside of the document directory even though it is stored in an encrypted format.

Caution: Encourage your users to use a different password for your web site than for other more essential things. For example, many people tend to use two passwords - one for all of their extremely important things, such as the login to their desktop computer, and for their bank account, and another for less sensitive things, the compromise of which would be less serious.

To create the password file, use the htpasswd utility.

To create the file, type:

```
htpasswd -c /usr/local/apache/passwd/passwords username
```

htpasswd will ask you for the password, and then ask you to type it again to confirm it:

```
# htpasswd -c /usr/local/apache/passwd/passwords rbowen
New password: mypassword
Re-type new password: mypassword
Adding password for user rbowen
```

The -c flag is used only when you are creating a new file. After the first time, you will omit the -c flag, when you are adding new users to an already-existing password file.

htpasswd /usr/local/apache/passwd/passwords sungo

The example just shown will add a user named sungo to a password file which has already been created earlier. As before, you will be asked for the password at the command line, and then will be asked to confirm the password by typing it again.

Caution: Be very careful when you add new users to an existing password file that you don't use the -c flag by mistake. Using the -c flag will create a new password file, even if you already have an existing file of that name. That is, it will remove the contents of the file that is there, and replace it with a new file containing only the one username which you were adding.

The permissions of the file should be set as follows:

```
chown root.nobody /usr/local/apache/passwd/passwords
chmod 640 /usr/local/apache/passwd/passwords
```

Set the configuration to use this password file

Once you have created the password file, you need to tell Apache about it, and tell Apache to use this file in order to require user credentials for admission. This configuration is done with the following directives:

AuthType   Authentication type being used. In this case, it will be set to Basic
AuthName   The authentication realm or name
AuthUserFile   The location of the password file
AuthGroupFileThe location of the group file, if any
Require   The `requirement(s)` which must be satisfied in order to grant admission

These directives may be placed in a .htaccess file in the particular directory being protected. If an .htaccess file alread exists with other settings append these directives to that file.

The example shown below defines an authentication realm called ``Restricted''. The password file located at /usr/local/apache/passwd/passwords will be used to verify the user's identity. Only users named rbowen or sungo will be granted access, and even then only if they provide a password which matches the password stored in the password file.

```
AuthType Basic
AuthName "Restricted"
AuthUserFile /usr/local/apache/passwd/passwords
Require user rbowen sungo
```

The phrase ``By Invitation Only'' will be displayed in the password pop-up box, where the user will have to type their credentials.

The next time that you load a file from that directory, you will see the familiar username/password dialog box pop up, requiring that you type the username and password before you are permitted to proceed.

Note that in addition to specifically listing the users to whom you want to grant access, you can specify that any valid user should be let in. This is done with the valid-user keyword:

Require valid-user

Optionally, create a group file

This is handled using authentication groups. An authentication group is, as you would expect, a group name associated with a list of members. This list is stored in a group file:

```
/usr/local/apache/passwd/groups
```

The format of the group file is exceedingly simple. A group name appears first on a line, followed by a colon, and then a list of the members of the group, separated by spaces. The current groups are:

level1: user admin level2: admin

Once this file has been created, you can Require that someone be in a particular group in order to get the requested resource. This is done with the AuthGroupFile directive, as shown in the following example.

AuthType Basic AuthName ``Restricted" AuthUserFile /usr/local/apache/passwd/passwords AuthGroupFile /usr/local/apache/passwd/groups Require group level2

The authentication process is now one step more involved. When a request is received, and the requested username and password are supplied, the group file is first checked to see if the supplied username is even in the required group. If it is, then the password file will be checked to see if the username is in there, and if the supplied password matches the password stored in that file. If any of these steps fail, access will be forbidden.

Password Protecting Directories

The Most Common Problems

- Description
- Discussions
- Search

Description

Here are some of the more likely problems with their solutions.

The web server error log is at /var/log/httpd/error_log. If you suspect that the web server has gotten into a bad state, restart it by typing ``/etc/rc.d/init.d/httpd restart" (as the root user).

Discussions

The discussions system is highly reliable. It's possible to make mistakes when setting up a discussion for the first time, but once it is set up there should be few problems.

Notification is the most likely source of problems, because it is the most complicated function. Check for the existence and permissions of the /var/log/subscriptions directory and its two log files, ``notify_log" and ``subscribe_log". These files must exist and be writable by the web server (user ``nobody").

If e-mailing answers to Ask an Expert or Problem Simulation submissions is not working, go to the discussion office and follow the ``edit" link next to the discussion. Make sure that the e-mail address from which reply messages are sent is valid.

Search

If you search for something that you know exists on the site and the search does not find it, then search is not working.

The most likely cause is corrupted search indexes. Follow the instructions under ``Search : Site : Administering the Site Search" to manually rebuild the indexes.

Another likely cause is corrupted permissions. The search index files must be readable to the web server, under user ``nobody".

Discussions Overview

- Description
- Discussion Office
    - o Viewing Discussions
    - o Creating a Discussion
    - o Editing a Discussion
- Office View of a Discussion
- The Limbo Discussion
- The Test Discussion

Description

The discussions system handles the general discussion, the Ask an Expert service, and the Problem Simulation service. When community discussions existed, it handled them too. This document provides basic information that pertains to all of these areas. There are separate documents about Communities, Ask an Expert, and Problem Simulation.

Discussion Office

The discussion office, available as a link (``View or Edit All Discussions") from the Office page, allows an administrator to view all discussions, create discussions, change discussion options, and edit or delete messages.

Viewing Discussions

The discussion office shows a view of all discussions that exist. The discussions are organized into a tree structure: There is a root discussion which is the topmost parent. Discussions named ``Root Something" are not real discussions, but are only placeholders which other discussions are attached to as children. In the view of discussions, notice the ``."'s which indent discussion names to indicate parent-child relationships between discussions.

From left to right, the columns in the office view of discussions are: (1) ``main", the main view of the discussion. This is the view seen by the public, in the case of public discussions. (2) ``edit", the link the change the discussion's options. (3) ``activity", the date of the most recent message. (4) ``discussion", the office view of the discussion (see below). (5) ``started", the date that the discussion was created. (6) ``#", the number of messages in the discussion.

Creating a Discussion

Follow the ``create a new discussion" link and fill in the discussion name (the name which is used in URLs), the human name (the full name for readers), and the short name (a name used instead of the full name where brevity is necessary).

The discussion will be created with notification turned off. See ``Editing a Discussion'' if you want to turn on notification.

Editing a Discussion

The ``edit'' link lets you change the options of a discussion.

You can change the parent and the names of the discussion. You can set the e-mail address from which messages are sent when replying to Ask an Expert questions or Problem Simulation answers.

You can also turn notification on or off. When notification is on, the discussion has a ``sign up for e-mail notification'' link which visitors can follow to sign up for notification. When a post is made to the discussion, those who are signed up receive e-mail notifying them of the new message. When notification is off, the link disappears and notification e-mails are not sent.

Office View of a Discussion

The office view of a discussion gives an administrator power to control the contents of the discussion. To reach the office view, follow the ``discussion'' link from the discussion office.

The office view of the discussion is similar to the main view, except for the extra administrator controls. These controls are: (1) On a topic page, there is a ``Delete Topic'' button. Press it, and the the topic will be deleted immediately. (2) On a message page, there is a ``Delete Message'' button which deletes the message. (3) On a message page, there is an ``Edit Message'' button which lets you change the author, author's e-mail address, subject, and body of the message. (4) On a message page for a message that is among others in a topic, there is a ``Split Off into New Topic'' button. This button pulls the message with its replies out of its topic and makes it into a new topic in its own right. Splitting a topic is useful when the discussion participants go off on a tangent.

The Limbo Discussion

Deleted topics are not actually deleted, they are moved to the Limbo discussion where they are invisible except to administrators. This is the only purpose of Limbo.

Deleted messages are completely deleted from the database.

The Test Discussion

There is a testing discussion that you can try stuff out in. This discussion is visible only to administrators, and it doesn't do anything important, so you can feel free to experiment with it.

USAMRMC Log No.: 02101001

Discussions Overview

Communities

- Description

Description

Originally, the site plan called for support for any number of communities. Each community would have its own discussion and its own Ask an Expert answer archive.

This facility has been removed, by request.

Communities

Ask an Expert

- Description
- Archived Answers
- Asking Questions
- Answering Questions
- Publishing Answers

Description

The Ask an Expert service allows visitors to ask questions which the staff may then choose to answer. Questions and answers which are generally interesting can be posted to a public archive of answers.

The service is implemented as a set of discussions. A question is treated as a message posted to an internal discussion that only the staff can read. Any answer is sent by e-mail. The answer archive is also a discussion, which is set up so that visitors can only read, and not post.

Archived Answers

There is one archive of answers. The link to the archives are above the question-asking form. That encourages visitors to look first and ask questions later.

Originally, the plan called for there to be one archive of answers for each existing community. This facility has been removed, by request.

Asking Questions

Visitors post their questions through a web form under ``Ask an Expert''.

Answering Questions

From the office page, follow the ``Answer Questions'' link (or, from the discussions office, follow the ``main'' link for the ``Ask an Expert'' discussion). This takes you to a discussion which only staff members can see.

To answer a question, read the question and follow the ``reply to this message'' link. If you check the ``e-mail your reply to the original poster'' box, your answer will be sent by e-mail. For internal discussion amongst the experts, don't check the box.

To publish a question and the answers it has accumulated, go to the question's topic page. There is a button at the bottom, ``Publish this topic."

Click that button, and the entire topic, the question and all its answers, will then become accessible to visitors through the answer archive. You may want to use the discussion office functions to delete extraneous messages and clean up the answer when you publish it.

You can only publish a question which has an answer.

Ask an Expert

Problem Simulation

- Description
- Replying to Answers
- Setting Up a New Problem Simulation
    - o Creating The Discussion Topic
    - o Creating The Problem Form

Description

The problem simulation system includes answer forms which visitors may fill in and submit. Staff may then review visitor answers and reply, creating a mentoring relationship.

Behind the scenes, problem simulation relies on the discussion system. The visitor's answers are concatenated into a single text message, and this message is posted to a private discussion, visible only to staff. Each problem posts to a specific, pre-created topic of the discussion.

Replying to Answers

From the main office page, go to Answer Problem Simulation Submissions. Problems are listed in order of most recent post, giving you some idea of where new answers have been posted.

To make a reply, simply reply to a posted message. To send the reply to the original asker, check the ``send e-mail" checkbox next to the submit button.

Setting Up a New Problem Simulation

There are two parts, setting up the problem form, and setting up the discussion topic for answers.

Creating The Discussion Topic

Post an empty message to the Problem Simulation discussion, at the top level. Its subject should be the problem name, so that staff members can keep things straight.

Click on the message to view it. The URL in your browser will have a number at the far right. Write this number down; you'll need it for the next step.

Creating The Problem Form

Now you need to make a problem form which posts answers to the topic.

The easiest way to do this is to copy an existing form. Change the question and answer boxes as appropriate.

Somewhere in the form will be a hidden field named ``thread_n'' whose value is a number. Change this number to the topic number you wrote down above. That's all.

Problem Simulation

Browsing the Document Library

- Description
- Starting
- Main Page
    - o Entire Library
    - o Categorized Library
    - o Selecting Items

Description

This file covers browsing the Document Library.

Starting

Click Document Library on the left panel. This takes you to the Document Library main page.

Main Page

The user is given a ``simple" search box (see documentation on Searching)

They are also shown a list of the Main Topics (category1 headings or bold links) that are ordered by rank. The user also has the option of expanding the tree to view the entire library. (see documentation on Catalog for description of structure)

Entire Library

If the user clicks ``View Entire Library" from the main page they are taken to another page which displays the tree structure. They can click on any of the Main Topics (bold links) to take them to a page showing only that topic and its subtopics.

Categorized Library

If the user clicks any of the Main Topics (bold links) from the main page (or the Entire Library page) they will be taken to a new page that contains only that topic and its subtopics.

Selecting Items

Whenever the user is presented with a plain link from the tree it is an element from the Library. This includes: Documents, Images, External Links. Clicking a Document Link, or Image will open a page to display detailed information on that item. (See documentation on Library Item Display)

Microsoft Access Files

- Description
- Overview of the Files
  - o bio05.mde
  - o bio05.mdb
  - o localdata
- Installation
  - o File Copying
  - o Linking Files
- File Backup/Relocation/Recovery
  - o Moving the files
  - o Backing up
    - Original Files
    - Data
  - o Recovering
    - Recovering the Original Files
    - Recovering the Data

Description

This documentation covers the MS Access files: Overview, Installation, Backup, Recovery

---

Overview of the Files

bio05.mde

bio05.mde is the front end file, it is the file that will be opened for data entry. bio05 contains forms and tables that are linked to localdata. bio05 itself does not contain any catalog data. The data is stored in localdata

bio05.mdb

bio05.mdb does not need to be installed on the machine. It should be kept as a backup. bio05.mdb is the source file used to make bio05.mde. It contains all the code. To convert bio05.mdb into bio05.mde click Tools -> Database Utilities -> Make mde file... Then save it. This compiles all the source code. The mde file is used because it is smaller, faster and will not put the user into debug mode if an error should occur. All following references to bio05 refer to bio05.mde (the compiled database file).

localdata

localdata.mdb contains the tables with the catalog data for bio05 and should not be changed or moved once it is installed.

File Copying

There are two files that need to be on the local machine:

```
bio05.mde
localdata.mdb
```

These files must be placed in C:/Program Files/biodefense They must also be able to write to this directory.

The location of these files should not change or it will be necessary to link the files again.

Linking Files

Once both files are copied you will need to link them together.

```
open bio05.
```

(You may be presented with the main form which may maximize itself, if so move it aside)

```
In the database view, click the "Tables" tab.

Verify that there are no tables currently linked.

From the main menu click:
 Insert -> Tables

Select "Link Tables"

Navigate to the localdata.mdb file, Select it

Click "Select All"

Click OK
```

The two files are now linked. You can now create the catalog.

MS Access stores the complete path of linked tables. This means that if a backup or file relocation occurs the files may not be linked correctly. The original localdata could be pointed to by both bio05 files or the link might be completely broken. It is not always apparent which files are linked therefore it is advisable to keep one copy in one place on one machine. Backups and file relocations should be carried out as follows:

Moving the files

If the file need to be moved make sure they are linked after the move. Re-link the tables by deleting the current ones in bio05 and following the linking procedure (See Linking Files)

Backing up

Backup's of both the data and the skeleton (original) files should be made.

Original Files

Keeping the skeleton files on disk is recommended. Take care not to keep the empty files in a place or state in which they could be confused with the live files. (See Linking Warning Note File Backup or Relocation)

Data

Backing up of the data can be accomplished by backing up only the localdata.mdb file.

Recovering

Recovering the Original Files

If for any reason a recovery of the original files is needed close and remove both bio05 and localdata, follow the instructions for Installation. This will leave you with a clean slate. For data recovery see below. (Recovering the Data)

Recovering the Data

If a recovery of the data is required exit Access, replace the localdata file that is in use with the backed up localdata. The name and path must match. Open bio05.

Microsoft Access Files

Document Library Catalog

- Description
- Creation
    - Enabled Fields
        - Style
        - Category1
        - Rank1
    - Disabled Fields
        - ID
        - Category2 - Category5
        - Rank2 - Rank5
    - Hidden Fields
        - Title
        - Image*
        - Document*
        - External Link*
        - Author
        - AuthorEmail
        - ContentProvider
        - CPEmail
        - CreationDate
        - Keywords
        - Description
        - CimercID
    - Tree Generation
    - Deleting Records
- Exporting
- Uploading
- Troubleshooting
    - The Document Library main page has an internal error:
    - The order is not correct:
    - The item is too far over:
    - Exporting does not take place:
    - Error on opening bio05:

Description

The library catalog is a hierarchical structure that displays the contents of the library. The catalog is created with the Microsoft Access database. It is then exported and uploaded to the website.

Once the files have been installed you can start to create the Catalog.

When the database (bio05) is opened the form for data entry is displayed (frmResources). This should be the only method for data entry, access to other tables is not required. All of the fields needed are available on this page, however they are hidden or disabled until needed. There are a number of fields that are immediately visible and enabled:

Enabled Fields

Style

Selection box for the style of the entry: (Heading, Document, External Link, Image). Heading is selected by default. Changing the style makes other fields appear.

Category1

The text from the category boxes is what gets displayed in the Document Library page. (See Tree Generation notes below)

Rank1

The rank of the category determines the order of display. (See Tree Generation notes below)

Disabled Fields

ID

Each entry gets it own unique ID. This field is filled in automatically and requires no user intervention.

Category2 - Category5

Categories 2 through 5 can only be filled in if the category before it is filled in.

Rank2 - Rank5

A rank can only be filled in if its category is enabled.

Hidden Fields

These fields will be displayed when ``style" is changed from Heading to any other style.

Title

This field is used for searching, it is the title of the resource. It is case insensitive and is displayed when an item is viewed.

Image*

The filename of the image that has/will be uploaded. The text must match the filename exactly.

Document*

The filename of the document in that has/will be uploaded. The text must match the filename exactly.

External Link*

The URL, can be link to a document or an external web site. It must be a full link (i.e. http://www.google.com instead of www.google.com)

Author

The name of the Author if applicable. This is a composite field.

AuthorEmail

The email address of the Author. This is a composite field.

ContentProvider

The name of the content provider. This is a composite field.

CPEmail

The email address of the content provider. This is a composite field.

CreationDate

A date may be entered. It must be in mm/dd/yyyy format. This is an optional field.

Keywords

Keywords used for searching. Case insensitive. Displayed with document display on web page. This is an optional field.

Description

A description of the item. Case sensitive searching.

CimercID

This is an optional text field.

* Only one of these is displayed depending on the style

Optional fields are only displayed on the web page if present. Presence is determined by non-null values. Therefore if there is no Author, entering spaces or ``---'' will cause the field to show with that value.

Composite fields are optional fields that are displayed on the web page in the same location as another field. For instance if a document has an author and the author's email is entered. The author's name will be displayed in its normal place and will be a hyperlink to his email. If there is no email it will be displayed as normal. If there is no author name yet an email is entered the field will be a link to the email with the email address as the text.

See Library Item Display for more information on optional and composite fields.

Tree Generation

```
Example outline:

   Introduction              (H)
     Who Are We?             (D)
     FAQs                    (L)
     Mission Statement       (D)
     Our Logo                (I)
   Biodefense                (H)
     Cimerc Home             (L)
     Resources               (H)
        phil.cdc.gov         (L)
        biodefense bible     (D)
```

This example outline will be used to illustrate the creation of the Catalog. The letters denote the document type and are not part of the outline:

```
   H -> Heading
   D -> Document
   L -> Link
   I -> Image
```

Each line of this outline is an entry in the access database and has a unique ID. There are two main topics (or Category1's):

```
Introduction
Biodefense
```

There are 6 secondary topics (or Category2's):

```
Who Are We?
FAQs
Mission Statement
Our Logo
Cimerc Home
Resources
```

There are 2 tertiary topics (or Category3's):

```
phil.cdc.gov
biodefense bible
```

This example only has 3 levels of depth, it is possible to have 5.

Both category1's are headings. It is possible to have the Category1's be a different style however this is not recommended because category1's that are headings are displayed on the main Document Library page as links to their own page. Changing their style may stop them from showing up in the Document Library main page.

To insert ``Introduction'' into the Catalog we set the following values on the form:

```
Category1:    "Introduction"
Rank1:        10
Style:        Heading
```

Style normally defaults to Heading.

Rank1 can be set to any reasonable integer value. Its purpose it to give order to the tree. The order of entry does not matter. All category1 items will be displayed in order of Rank1. So it is necessary to give it a value lower than the ``Biodefense'' topic. It is advisable to give items ranks that are separated by more than 1. This allows you to insert topics after most of the Catalog is created.

After entering the previous values, pressing the ``next'', ``new'', or ``export'' buttons will save the record.

```
Example values "Biodefense"

Category1:    "Biodefense"
Rank1:        20
```

```
Style:        Heading
```

To create the ``Who are we?'' entry enter the following values in a new record.

```
Category1:    "Introduction"
Rank1:
Category2:    "Who are we?"
Rank2:        10
Style:        Document
```

Once you change the style to document, many other fields appear. Fill in some values for these fields, not all are required. (See Enabled Fields description above)

When entering the data for Category1, the form should autocomplete your entry after you type the first few letters. Alternatively you may press the drop down box to select ``Introduction''. It is necessary to include the category1 (or any other preceding categories) so the current entry can be associated with its ``parent'' and be displayed under it.

Rank1 remains blank. The rank is filled in on the lowest category value.

Category2 is the text to be displayed for the current entry.

Rank2 is required to indicate the priority in this subsection. Rank2 is only compared to other Rank2's under the same section. Therefore this Rank2 will have to be smaller than ``FAQs'', ``Mission Statement'' and ``Our Logo''. It does not conflict with or compare to any Rank1, 3, 4, 5.

Deleting Records

Entire records may be deleting by pressing the ``trash'' icon.

If the item is a heading it will ask you if you are sure you want to delete it.

If the item is an image, document or link. You will be prompted to delete the corresponding record from the appropriate table.

Clicking yes to the above prompt will delete associated records. You will then be prompted to delete the current record as usual.

If you do not click yes to delete the corresponding record you will not be allowd to delete the current record

Once all the entries have been made, the file will need to be exported. Clicking the export button creates a file called export.txt in <Drive>:/Program Files/biodefense

This file can then be uploaded.

Uploading

To upload the catalog, open a browser and go to www.site.com/bio/office/uploadCatalog.html.

Click browse, navigate to <Drive>:/Program Files/biodefense select export.txt, Click OK, Click Submit.

A page should display stating that the Document Library has been updated.

This can be verified by clicking the ``Document Library" link and examining the updates.

Troubleshooting

The Document Library main page has an internal error:

Make sure there are no blank records in the Catalog, specifically check the last record to make sure it has no ID. The ID field should say <autonumber>. If it, or any other record, is blank it should be deleted. (See Deleting Records)

The order is not correct:

Make sure the items that appear out of order have ranks. If they do not they will filter to the extremities of the tree. Also make sure the out-of-order item has a valid ``parent" topic.

The item is too far over:

A level may have been skipped in the data entry. Make sure this item has a ``parent" topic

Exporting does not take place:

Make sure the C:/Program Files/biodefense directory exists and it is able to be written to.

Error on opening bio05:

``Form cannot be displayed"/``Tables not available"

Make sure the files are correctly linked. Check to see if localdata exists. See Installation documentation under MS Access File.

Document Library Catalog

Library Item Search

- Description
- Search Options
    - Search Text
    - Search Location
        - All*
        - Title
        - Keywords
        - Description
        - Author
    - File Type
        - All*
        - Images
        - Documents
        - Links
    - Sort Order
        - Title*
        - Description
    - Items Per Page
- Search Types
    - Simple Search
    - Advanced Search
- Search Results
    - Re-Search Options
    - Sort Options
    - Current Item Display
    - Library Results
    - Page Navigation

Description

The library search queries the contents of the Document Library (see Catalog Documentation).

Search Options

Defaults have a '*' next to them:

Search Text

Text to be searched for. Can query ``%" to retrieve all items. 50 character maximum. Leading, trailing and multiple spaces are removed. Case insensitive (except for Description) Multiword searches are possible.

Search Location

The meta-data to search for. Currently includes:

All*

Searches title, keywords, description, and author for matches.

Title

The document title is matched against the search string, this should typically be the same as the category entry that is displayed in the Document Library browsing.

Keywords

A list of keywords that may be present

Description

Searches match against description. This search is case sensitive.

Author

Searches against Author name if available

File Type

The search can be restricted to files of the following types:

All*

No restriction, all matches are returned

Images

Only images are queried, returned

Documents

Only documents are queried, returned

Links

Only links are queried, returned

Sort Order

Title*

Default sort order. Sorted alphabetically by title, regardless of file type.

Description

This sorts by File Type then alphabetically by title.

Items Per Page

Determines the number of items per results page. Current values (5, 10, 15, 20)

Search Types

There are two library search types available: simple and advanced. The main difference is the display. Both have the same default options (see Search Options).

Simple Search

Simple search is a ``one line" search. It is displayed as a text field, a search button and a link to the advanced search. It uses all the default values.

Advanced Search

Advanced search displays all available options. All default values are initially selected.

Search Results

After clicking search the user is taken to a page where the results are displayed. They are shown the text they searched for in quotes. They are given a simple search box to search again. They are given some ``re-search" options depending on their previous search.

Re-Search Options

Re-Search options will either limit or expand the previous search depending upon the search criteria and results:

```
 If there were results:
    If the user searched for everything:
        They are given the option to limit results
    If the user searched for a specific type:
        They are given options to change results to other or all types
```

USAMRMC Log No.: 02101001

F-90

```
If there were no results:
    If the user searched for everything:
        No results are displayed
    If the user restricted the search (file type):
        The user is given options to expand the search
```

Sort Options

The user is given the option to change the current sorting mode.

Current Item Display

The user is shown which items are being displayed on the current page in the format of:

```
Displaying items 1 through 5 of 26
```

Library Results

5 results are displayed unless the user changed the items per page option.

See documentation on Library Item Display for more details.

Page Navigation

The user is given links to go to any page in the results. The current page is bolded.

Library Item Search

Library Item Display

- Description
- How Items Are Displayed
- More Object Specific Displays
  - o Documents
  - o External Links
  - o Images

Description

This file outlines how items in the library are displayed. They are viewable by browsing or searching (see documentation on Browsing/Searching). Browsing returns one item at a time. Searching may return multiple items. The items that can be displayed are:

Documents

can be displayed from browsing or searching

Images

can be displayed from browsing or searching

External Links

can be displayed from browsing or searching.

How Items Are Displayed

Every item in the library has certain meta-data associated with it. A image may have an author, creation date, CimercID, etc. Some of the meta-data is optional, some is composite. See the tables below:

Basic layout of table for displaying any item in the Library:

```
| 0          | 1                          |
| 2          |                            |
| 3*         |                            |
| 4*         |                            |
| 5          |                            |
| 6          |                            |
|_7_____|_____|
```

Each number represents a field in the table

USAMRMC Log No.: 02101001

Depending on the type of library item (Image, Link, Doc) fields get different values. When an image is going to be displayed then field 1 is the image. For documents and other ``non-images'', field 1 is the description

```
Current settings:

Field   :  Value           :Composite:Optional:   When
---------------------------------------------------------------
0       :  Title           :         :  no     :  Always
1       :  Image           :         :  no     :  Images
1       :  Description     :         :  no     :  non-images
2       :  URL(download)   :         :  no     :  documents
2       :  URL(link)       :         :  no     :  links
2       :  Description     :         :  no     :  images
3       :  Author          :  yes    :  yes    :  Always
4       :  ContentProvider:  yes    :  yes    :  Always
5       :  CreationDate    :         :  yes    :  Always
6       :  CimercID        :         :  yes    :  Always
7       :  Keywords        :         :  yes    :  Always
```

Optional fields: if they are present they are displayed, if they are NULL (e.g. no text) they do not get written into the table. Fields which are not optional will display with their tag and have a blank value follow such as ``Title: '' ``Description: ''

Composite means the value may come from more than one field from the database. For instance field 4 can be the author's name, email address or both. For instance:

```
        case|  1   2   3   4    |
            |-------------------|
      author|  no  no  yes yes  |
 authoremail|  no  yes no  yes  |
            |-------------------|
```

In case 1, nothing is provided (both fields are blank in the database) therefore field 3 will be completely omitted, as opposed to having a Null value appear

In case 2, only the authoremail is provided therefore the field will show the author's email address in that field which is a hyperlink to the same address.

In case 3, only the author's name is provided therefore the field will be regular text of the author's name.

In case 4, both are provided and the text will the author's name that is a hyperlink of his email address.

Documents

Documents will be displayed after searching or by clicking a document in the Document Library. The user can download the document by clicking ``Download" or by right clicking ``Download" and pressing ``save target as..."

External Links

External Links can be viewed as a library item by searching or browsing. Clicking an external link while browsing the Document Library will take the user to a page to view the details of that link. Links display their address as a hyperlink and will open in the current window.

Images

Images will be displayed after searching or by clicking an image in the Document Library. Image width is restricted in this view to prevent the page from becoming too wide. The image itself is a hyperlink to a page where the image can be viewed at full size.

Library Item Display

Search Overview

- Description
- Search Types:
  - o Site Search
  - o Discussion Search
  - o Library Search
- All-In-One Search:

Description

This document explains the three distinct searches: Site Search, Discussion Search, Library Search. It also explains how the ``basic" search works to tie all three together. Detailed documentation on each search is also available.

Search Types:

Site Search

The site search searches the static pages. This primarily includes all html files under the content directory. This is a glimpse search.

Discussion Search

The discussion search searches all public discussions. This includes discussions under Community Discussions (community-root), Expert Answer Archives (expert-root) and General Discussion (general). This is a glimpse search.

Library Search

This search covers the Document & Image Catalog.

All-In-One Search:

The All-In-One search is a ``simple" search box that searches all three distinct searches and brings back results for each. BASEURL/search/ brings up this search.

There are links to switch to a specific search if the user knows specifically what they are looking for. This search uses modified control files and describers (See Administering Site Search) to limit the amount of results. The results are capped at 5 for each distinct search.

The search options that are used are the defaults for each individual search.

USAMRMC Log No.: 02101001

The same preprocessing is done for these searches as for the individual ones.

Search Overview

Administering the Site Search

- Description
- Searching Basics
  - Indexing
  - File Relocation
  - Executing
  - Preprocessing
- Preprocessing
- Specifying Search Locations
- Control Files
- Describers
- Directories
  - Search (/var/www/html/)
    - .mc
    - display_components/
  - Search (/var/www/)
    - indexes/
- Files
  - crontab
  - files.sh
  - reindex
  - .glimpse_*
  - index_copy.pl
  - page_results.html
  - searcher
  - preprocess_search
  - pages.search.ctrl
  - glimp_search
  - pages_item_list

Description

The site search finds ``html'' documents under the content directory and allows users to search these documents. This document describes how to set up the site searching.

Searching Basics

Indexing

In order to perform a search quickly work is done beforehand to find out where everything is. An indexer goes through all of the files specified (Specifying Search Locations) and builds statistics on its contents. Indexing is typically done by a cron job (crontab). It should be done when the

site traffic is low. In order for new content to be searchable the indexer must be run after the content is added.

File Relocation

Indexes are built in one location and moved to another. (indexes/) This is done by index_copy.pl.

Executing

A search is executed when the user presses the search button. The search uses the previously built index and returns the matches.

Preprocessing

Preprocessing

The search text is cleaned up before the search is carried out. This removes common words such as ``as", ``the", etc. It also removes question marks and extraneous spaces. The user is notified of corrections made to their search. A search for ``what is biodefense?" results in items containing ``biodefense". The other words are trimmed off.

Search Correction/Cleanup

The preprocessing is handled by preprocess_search.``

Specifying Search Locations

Specifying locations that will be searched is done in files.sh.

Control Files

The control file is where the settings of the search are specified. See pages.search.ctrl.

Describers

The describer contains the settings for formatting the output of the search. See pages_item_list.

Directories

There are two directories where search files are located.

Search (/var/www/html/)

This directory located under /var/www/html/ contains pages for displaying the results, describers and snippets

.mc

Location: /var/www/html/search/.mc/

This directory contains a few scripts used for searching (See Files Below)

display_components/

Location: /var/www/search/display_components

This directory contains methods for displaying the page.

Search (/var/www/)

This directory located under /var/www/ contains scripts, and directories for generating, moving and holding the indexes.

indexes/

Location: /var/www/html/search/indexes/

This directory holds all of the current indexes.

Files

crontab

This file specifies when indexes are to be built. It is best to have indexes built when the site traffic is low. Indexing can also be done manually:

```
/var/www/search/re_index/pages/ L</"reindex">
/var/www/search/bin/ L</"index_copy.pl">
```

files.sh

Location: /var/www/search/re_index/pages/files.sh

This is a script that outputs the names and locations of all the files that are to be indexed. It currently finds all html files in the content directory. Subdirectories are also included:

```
find /var/www/html/content/ -name *.html
```

This script does not get called for indexing directly. It is called by reindex.

reindex

Location: /var/www/search/re_index/pages/reindex

This script creates the indexes. It uses files.sh to figure out which files are requested. It outputs the .glimpse_* files.

.glimpse_*

Location: /var/www/search/re_index/pages/reindex/.glimpse_*

A number of these files are created after running reindex. They are copied to the correct location by index_copy.pl.

index_copy.pl

Location: /var/www/search/bin/index_copy.pl

This script should be run after reindex is run. This script copies all of the .glimpse_* files to indexes/.

page_results.html

Location: /var/www/html/search/page_results.html

This file is where the results are displayed. It calls searcher.

searcher

Location: /var/www/html/search/.mc/searcher

This file calls the glimpse_search after it gets the control file pages.search.ctrl and after it calls preprocess_search.

preprocess_search

Location: /var/www/html/search/.mc/preprocess_search

This file returns the recommended search terms, the user explanation and abort_search.

The recommended search terms start off as the user input and get changed as appropriate. To add a word the the filter make an entry in the badTerms hash. This will then filter out that word and report the associated message with it.

The user explanation is the text that is displayed when a word has been filtered out.

pages.search.ctrl

Location: /var/www/search/ctrl

This is the control file. It is specified on the search page. The contents are:

```
Method: glimpse_file;
Index: pages;
Describer: pages_item_list;
Title: <BR><center><H4>From the CiMeRC Web Pages</H4></center>;
```

It chooses the index to use from the indexes/ directory.

It chooses the describer to use from the display_components/ directory

It also sets the title of the results page (page_results.html)

glimp_search

Location: /var/www/html/search/.mc/glimp_search

This file prints the top of the page then calls the appropriate display component (pages_item_list)

pages_item_list

Location: /var/www/html/search/display_components/pages_item_list

This file describes how the pages that are found should be displayed. It gets the top part of the page and displays it below the link to the page.

Administering the Site Search

Using the Site Search

- Description
- Search Options
    - o Search Text
    - o Search Type
        - Any Words*
        - All Words
        - Exact Phrase
    - o Match Type
        - Complete Words*
        - Parts of Words
    - o Buttons
        - Search
        - Reset
- Preprocessing
- Results
- Re-Search

Description

The site search returns pages that contain the search text.

Search Options

Defaults have a '*' next to them:

Search Text

Text to be searched for. 29 character maximum. Case insensitive. Multiword searches are possible. Text undergoes some Preprocessing.

Search Type

The way to search for the Search Text. Options:

Any Words*

Any of the words the user inputs are used to find results. (``OR" Logic)

All Words

Only results that contain all of the words are returned. (``AND" Logic)

Exact Phrase

The exact phrase is matched.

Match Type

This gives the option to search for complete words or to expand the search to words that contain the search text.

Complete Words*

A search for ``heal" matches only items that have ``heal" in them.

Parts of Words

A search for ``heal" matches ``heal", ``health", ``healthy", etc.

Buttons

Search

Starts the Search

Reset

Resets the default values.

Preprocessing

The search text is cleaned up before the search is carried out. This removes common words such as ``as", ``the", etc. It also removes question marks and extraneous spaces. The user is notified of corrections made to their search. A search for ``what is biodefense?" results in items containing ``biodefense". The other words are trimmed off.

Results

The results are displayed in a list. An element of the list contains a link which points to the page that matched. Beneath the link is the start of the page.

Re-Search

The user is given an option to search again with new text.

Using the Site Search

Registration

- Description
- Login & Registration Pages
- Form Submission, Logging, and the Index page
    - Login
    - Registration
    - Logging
- Database
- Forum::People module
    - Passwords
- Author

Description

The registration (and login) processes for the Self Assessment application.

Login & Registration Pages

The login page is here: content/selfAssessment.html. It is linked in the left navigation bar of the main site template.

The registration page is here: content/assessment/register.html. It is linked of the login page (see above).

Form Submission, Logging, and the Index page

Login and registration forms both submit to the index page.

Login

If the action is logging in, the index.html page calls the check_password function of the Forum::People module. A successful login results in the first page (the 'default' page) being displayed. An unsucessful login results in the login page being re-displayed with a small message noting an unsuccessful login.

Registration

If the action is a registration, the index.html page makes a component call to the save_reg component. This component calls the add function of the Forum::People module.

Forum::People::add returns 0 on failure or record_id number on success. The save_reg component returns an empty string on success or an error message string on failure to the index.html page. When the calling chain gets back to index.html, a successful registration ultimately results in the display of the first assessment page (the 'default' page). An unsuccessful registration should display an error message to the user.

Logging

All registrations, both successful and unsuccessful, should be logged to the web server error log. Successful registrations should also result in an email being sent to webmaster@cimerc.org. A successful login is also logged to the web server error log.

Database

Registration info saves to the people table of the people database. The people table schema is documented elsewhere. It can also be viewed in sqsh as follows:

```
sqsh> use people
sqsh> sp_help people
```

Forum::People module

The Forum::People module is located here:

```
/usr/lib/perl5/site_perl/5.6.1/Forum/People.pm
```

We use the Forum::People::add function in the save_reg component. We use the Forum::People::check_password function in the index.html component.

Passwords

When collecting a new password from the registration form, we use the field name 'clear_password', which signifies that the data is in clear text. When this info gets passed to the Forum::People::add module, the password data is encrypted and saved in the 'password' field and the 'clear_password' data is deleted.

For authenticating logins, the user-supplied password is encrypted and compared to the stored encrypted password.

Author

David Tristano, davidt@mathforum.org

Registration

New Pages and Maintenance

- Description
- Page Content Served via assessment/index.html
- Adding Question Pages
- Author

Description

Info for adding html pages, adding question pages, rearranging questions and answers.

Page Content Served via assessment/index.html

Most pages in the self-assessment application have their content called by the index page and served through the template provided by the index page. The template includes the beginning and ending html FORM tags as well as a hidden field with the value of $page set so that the next pages display in their correct order.

Adding pages to this setup involves editing the index.html page:

```
1.  Add a page title to the $page_titles data structure.
2.  Add an elsif case to the area labeled:  CHOOSE WHICH PAGE TO SHOW NEXT
```

Added pages need to include their own submit button and may need the js_submit javascript. See the content/assessment/default file for good examples of both the javascript and the submit button.

Adding Question Pages

Adding new question pages (Q_1, Q_2, ... Q_14, etc...) involves the following:

```
1.  Add rows to $pages_and_questions in the question_data file
    a.  the big-Q numbers must be consecutive starting with 1 (eg. Q_1,
Q_2...)
    b.  the little q numbers don't need to be consecutive, but
        they need to be unique (ie. don't reuse a question on another page.
2.  Add entries to $questions_and_answers in the question_data file
    a.  best to copy and paste an existing set of data
    b.  the first number to the upper left is the small q question number
    c.  the list of answer texts comes next
    d.  the list of answer numbers comes last -- these are the blurb
numbers
```

       e.   the answer numbers (blurb numbers) do not need to be unique --
            you are free to re-use the blurbs if you wish.
    3.   Add the question text to get_question_text
    4.   Add any new blurb texts to get_blurb_text
    5.   Add the recommended answers for new parent questions to get_answer_text

---

Author

David Tristano, davidt@mathforum.org

New Pages and Maintenance

Questions and Answers

- Description
- Display
- Pages, Questions, Answers, etc...
    - Pages
    - Questions (and Javascript)
    - Answers and Popup Blurbs
    - Recommended Answers
- Data
    - Pages & Questions
    - Questions & Answers
    - Question Texts
    - Recommened Answers
    - Blurbs
- Author

Description

An explanation of the question pages, questions, answers, popup blurbs, and recommended answers, including how to add and change questions.

Display

All question pages display though the content/assessment/question file, which is pulled up through a mason component call on the index page. If the user clicks the ``Continue" button from the default page, the question page is called and the first question is loaded into it. Subsequent clicks to ``Continue" will keep calling the question page until each question is displayed in turn.

Answering a question triggers a javascript to display a popup window named blurb.html. The contents of the popup window are the text of the blurb corresponding to the number of the answer given.

After the final question displays, a click to the ``Continue" button will call the 'done' page. As with the 'question' page, the 'done' page displays as a component call from index.html. From the done page, the user has the choice to review all their answers (handled by the 'results' component) or to compare their answers to the recommended ones (handled by the 'compare' component). It is on the compare page that the recommended answers are displayed.

Note: The displays of the 'results' and 'compare' pages are so similar that for simplicity all the work is really done by the results component. The 'compare' component is just a wrapper for 'results' which sets some configuration options. This is documented in the files themselves: content/assessment/results and content/assessment/compare.

USAMRMC Log No.: 02101001

Pages

At the time of this writing there are 14 question pages. To the user, these are presented as ``Questions" (for example, ``Question 1 of 14", ``Question 2 of 14", etc...) Each of these 14 question pages may in fact contain more than one question text. In other places in the documentation and in the perl files themselves, I sometimes refer to the 14 question pages as ``big Q" questions, and the individual question texts as ``little q" questions. This usage mirrors the way the html select fields and answer fields were named and numbered in the original .asp version of the assessment.

Note: The ``big Q" question pages must remain sequentially numbered with no questions skipped.

Questions (and Javascript)

At the time of this writing, there are about 25 individual question texts, often referred to as the ``little q" questions. There are one or more ``little q" questions on each ``big Q" page. For the purposes of one of the javascripts employed on the question page, the first ``little q" question on the page is referred to as the **parent** question. Subsequent ``little q" questions (if there are any) are referred to as the **children** questions.

On the question page, a javascript disables the ``Continue" button until all active questions have been answered. This javascript also disables the children questions until the parent question has been answered. In the current version of the assessment, if the answer to the parent question is ``no", the children remain inactive and the ``Continue" button activates.

Note: The ``small q" questions do not need to be numbered in any particular order and numbers may be skipped as well.

Answers and Popup Blurbs

The format of this assessment is multiple choice handled though html select fields. For each ``small q" question, there are two or more multiple choice answers (for example: ``yes", ``no", ``don't know"). For each answer, there is a corresponding numbered blurb. When an answer is selected, the text of the blurb displays in a popup window triggered by another javascript. The blurb display file is content/assessment/blurb.html

Recommended Answers

At the end of the assessment, on the 'compare' page, which is linked off the 'done' page, users get the chance to compare their answers to the recommened ones. In the .asp version of the assessment, only parent questions had recommended answers. Since the parent question is the first ``small q" question text on each ``big Q" question page, there is only one parent question per

page. Therefore there is only one recommended answer per page. For simplicity then, the texts of the recommended answers are keyed to the ``big Q" page numbers.

Pages & Questions

The lists of pages (big Q) and questions (small q) are contained in the file: content/assessment/question_data. There are two data structures (hashes) in that file. In the first hash, the keys are the names of the pages (big Q) and the values are lists of the (small q) question numbers that go on each page. The first small q question is the parent question, any subsequent questions are the children.

Questions & Answers

The relationships between questions (small q) and their answers are contained in the second hash in the content/assessment/question_data file. The keys to the hash are the question numbers. For each question, there is another nested hash containing the list of answer texts (eg. ``Yes", ``No", ``Don't Know") and a list of corresponding blurb numbers (eg. (4, 5, 6).

Question Texts

The actual text of the questions are contained in the file, content/assessment/get_question_text. The data is stored in a hash; the keys are the small-q question numbers.

Recommened Answers

The texts of the recommended answers are stored in the file, content/assessment/get_answer_text. The recommended answers are stored in two parts: the [yes/no/don'tknow] part, and the blurb part. For display purposes, the two parts are joined with a line break and displayed together. Only the parent question on a page gets a recommended answer. The data are stored in two hashes; the keys are the big-Q page names.

Blurbs

The texts of the blurbs are stored in the file, content/assessment/get_blurb_text. The data is stored in a hash; the keys are the answer numbers (blurb numbers) in the second hash in the question_data file

---

Author

David Tristano, davidt@mathforum.org

Questions and Answers

Site Map

- Description
- Map
- Control Flow
- Saving Data
- Question and Answer Data Structures
- Adding Pages
- Author

Description

Site map for the self-assessment application

The following lists the pages comprising the self-assessment and describes the control flow through the application.

Map

(If this ascii art diagram does not display in a fixed-width font, it may not make much sense.)

```
|    'login page'  |                                            .
|                  |                                            .
|                  |                                            .
| URL=content/sel  |                                            .
| fAssessment.html |                                            .
|         |      \                                             .
|         |       \ (need to register?)                        .
|       (login)    \                                           .
|         |         \                                          .
|         |          \ |    'reg page'  |                      .
|         |            |                |                      .
|         |            |                |                      .
|         |            | URL=content/as |                      .
|         |            | sessment/regis |                      .
|         |          / | ter.html       |                      .
|  _____/                                            .
| /                                                    . .
| |                                                          .
| |                                                          .
  \ | /                                                       .
|           |        |                  | copy.html          .
|  'index page'  |   | ----> |  'default    | _____/          .
|                  |        |   page'    |      \              .
| URL=content/asses|        |            |      ack.html       .
| sment/index.html |        |            |                      .
|                  |        |            |                      .
|                  |        | questions: |                      .
```

```
| NOTES: This page  |         |   Q_1     |                              .
| holds the template|  ---->  |    through|  _____(popup blurbs)        .
| for the remainder |         |   Q_14    |        (blurb.html)          .
| of the pages, but |         |           |                              .
| does not actually |                                                    .
| contain any con-  |                                                    .
| tent of its own.  |                                                    .
| The pages to the  |                                                    .
| right here should |         |           |         ___ results         .
| display in order  |         |  'done'   |        /                     .
| as the user clicks|  ---->  |           |  ___/___ compare            .
| the form submit   |         |           |        \                     .
| buttons.          |         |           |         \___ restart        .
|                   |         |           |                              .
```

Control Flow

All forms in the self-assessment application submit to the index page. The index page chooses what actions to take and what page content to display based on which form was submitted. Decisions are made based on the value of the hidden form field named 'page'.

The order of pages in the application is this: default page, question pages, done page. After the done page, there are three additional choices that may be taken. For those three, the index page knows what to do based on the value of $page and on the possible values of three variables named $goto_*

The majority of navigation through the application occurs through the form submit buttons, although there are a few html links as well. Access to the registration form for new users is through a link. Also on the first page of the assessment (the page named 'default'), there are two links: one to copyright info, and one to an acknowledgements list.

Saving Data

As the user clicks through the questions, answers are saved and passed along to the next page through hidden fields in the form. By the end of the assessment, all answers to all questions are saved and passed from page to page through these hidden fields.

At the end of the assessment is a final page named 'done'. This page contains three submit buttons which lead to three different followup activities. At this point the user may review all their answers or compare their answers to recommended ones. These activities should replicate the functionallity of the .asp version of the assessment.

Question and Answer Data Structures

See other documentation.

See other documentation.

Author

David Tristano, davidt@mathforum.org

Site Map

FORUM PRESENTATION

Biodefense Education Forum Prototype

Biodefense Education Forum: An Overview

www.cimerc.org
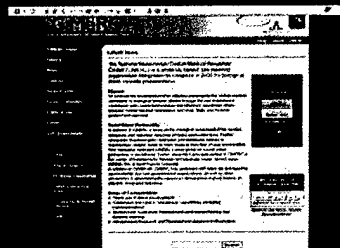
Final Report

CiMeRC

Biodefense Education Forum: An Overview
www.cimerc.org

CiMeRC

Presentation Table of Contents

Introduction

Objectives

Methods

Results

Conclusions

Final Report

CiMeRC

Forum Introduction

Supports web-based community interaction

Provides collaborative learning environment

Supplements traditional online learning

Promotes self-initiated learning

Constructs community/individual knowledge

CiMeRC

Forum Introduction:
Biodefense Community Design

Designed for multiple response sectors
·

Participating rural/urban expert groups
·
·
·
·
·
·

CiMeRC

Forum Introduction:
Proof of Concept

Math Forum's Math Education website
·
·
·
·

... "most successful educational Internet applications"

CiMeRC

Forum Objectives

Train for coordinated response

Develop and disseminate information

Remediate knowledge of individuals

Assess effectiveness of institutional response

Foster connections between sector-specific professionals

CiMeRC

Forum Methods

Technical development
.
.
.

Virtual community development
.
.

CiMeRC

Forum Methods
Technical Development, Platform Selection

Considered by Math Forum/CIMERC technical staff
.
.
.
.

CiMeRC

Forum, Technical Development
New Platform Compatibility

With existing Math Forum software

With HP servers (purchased by CIMERC)

With versions of one another

Operations and development staff familiarity

CiMeRC

Forum Methods
Technical Development, Configuration

Red Hat Enterprise Linux 2.1

Modules installed: perl, mason, glimpse...

Sybase Adaptive Server Enterprise 12.5
.

Security/server setup:
http://bioapp.cimerc.org/office/manual/html/SecuritySetup.html

CiMeRC

Forum Methods
Technical Development, Software

Foundation: Math Forum community/services software

Built customized
.
.

Adapted proprietary discussions software

CiMeRC

2

Forum Methods
Community Development Foundation

Prior Math Forum experience
- .
- .
- .

Receive help
Find challenging/interesting activities
Retrieve resources

CiMeRC
National Bioterrorism Civilian Medical Response Center

Forum Methods
Community Development, First Steps

Meet with Rural/Urban SMEs

Engage participants as motivated individuals
- .

Encourage private expert discussion

CiMeRC
National Bioterrorism Civilian Medical Response Center

Forum Results

Built server platform to house
http://www.cimerc.org

Redesigned (not graphical) CIMERC portal

Developed Website Construct for Civilian
Medical Emergency Response Community

Fostered nascent virtual community for
Biodefense Response Professionals

CiMeRC
National Bioterrorism Civilian Medical Response Center

Forum Results
Website Development

Commonalities among following slides
- .
- .

FAQs
Ask an Expert
Problem Simulation
Discussions
Library
- .

CiMeRC
National Bioterrorism Civilian Medical Response Center
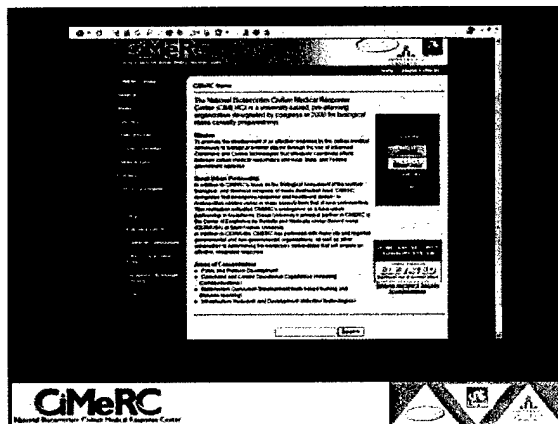
CiMeRC
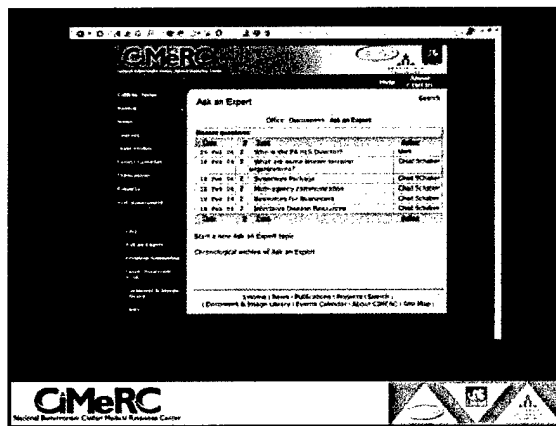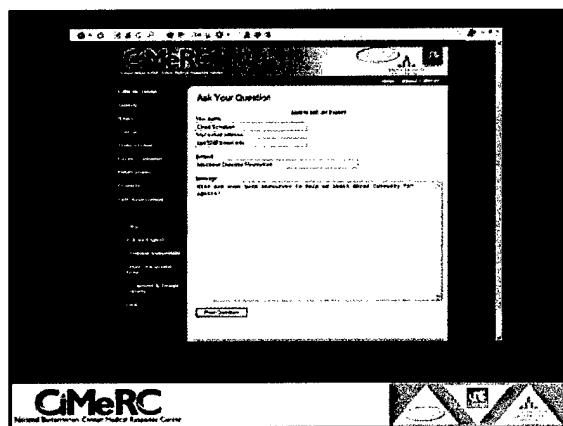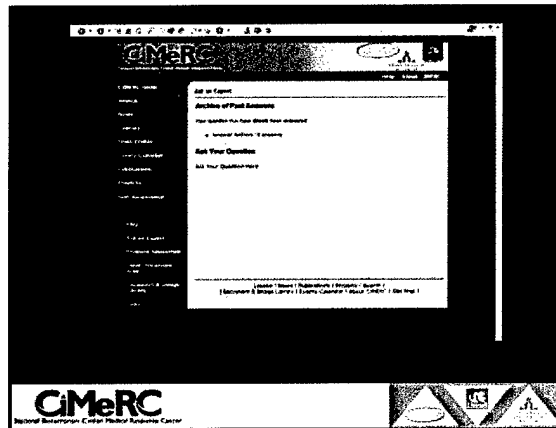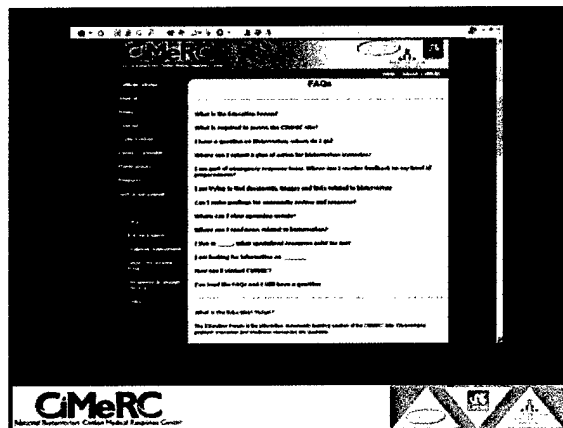National Bioterrorism Civilian Medical Response Center

---

Forum Results
Question and Answer

FAQs

Search Ask an Expert Archives

Pose question to Ask an Expert

Expert answers

Expert publishes, with permission

CiMeRC
National Bioterrorism Civilian Medical Response Center

Forum Results
Problem Simulation

User answers presented situations

Expert responds

Expert mentors user iteratively

Mentoring process is completely private

Future question: "Do we publish and add to the knowledge base?"
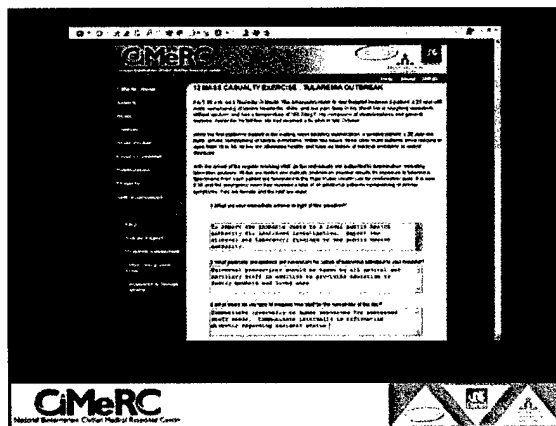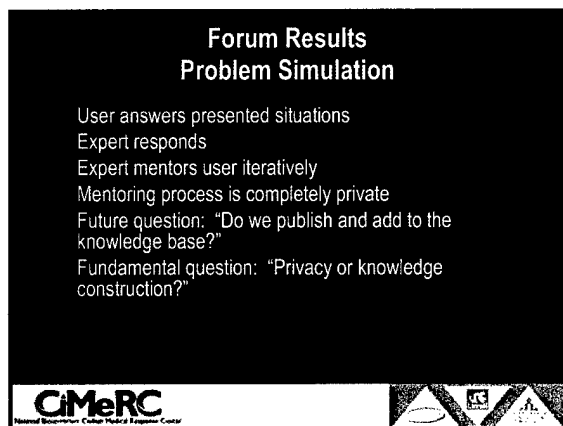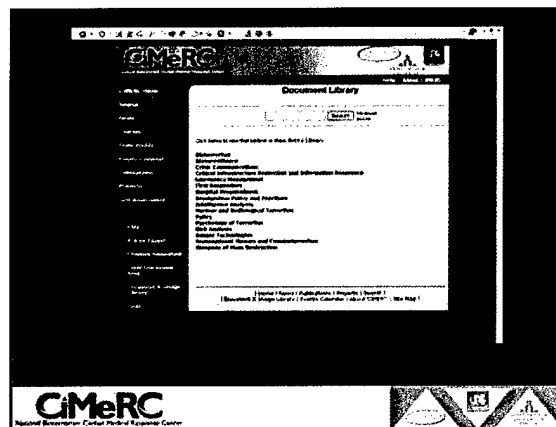
Fundamental question: "Privacy or knowledge construction?"

Forum Results
Document Library and Search

Library
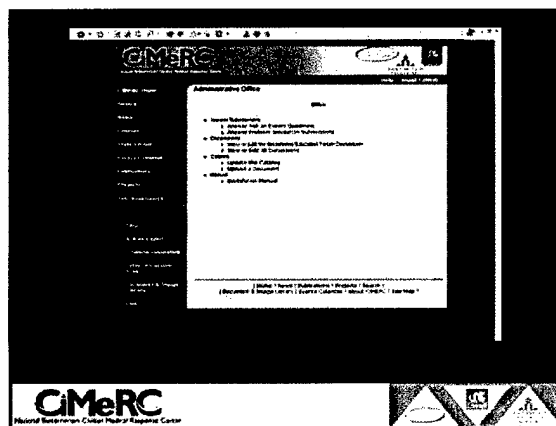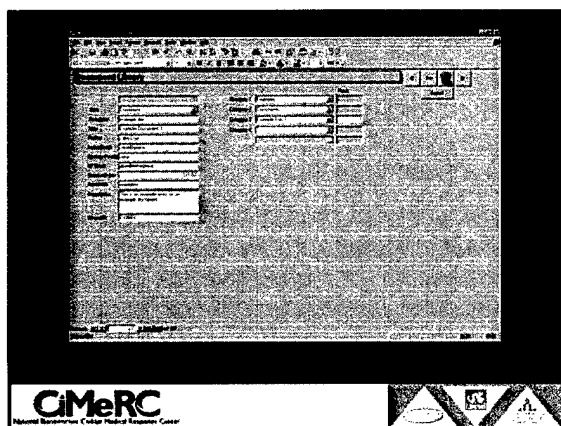
Search
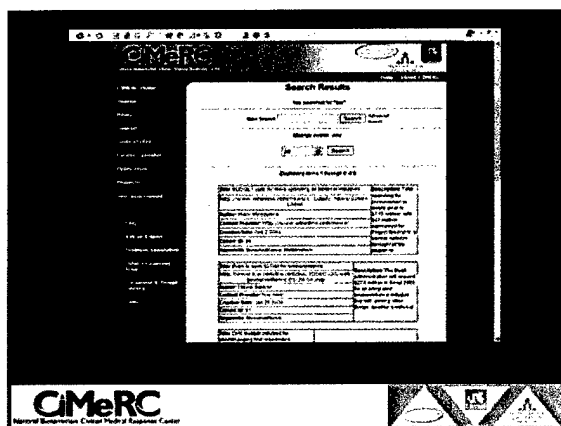
Forum Results
Office

Catalog resources on client
Upload resource metadata to server
Upload resource to server
Respond and/or publish

Facilitate discussions
Documentation for site

Forum Conclusions:
Future Developments

Extend to multiple biodefense communities
Continually assess community members' needs
Continually assess sponsor's learning needs
Respond to assessments
Improve/Extend site services from assessments

CiMeRC
National Bioterrorism Civilian Medical Response Center

Biodefense Education Forum Prototype
Final Report

Experience with first responders and key actors in planning and policy development has made clear the rapid evolution of information and knowledge about effective response to bioterrorism threats and incidents. In a context of significant change and somewhat independent, sector specific educational and policy initiatives, there is a critical need for a platform that facilitates learning and assessment across involved communities.

Click Here To View Entire Document

CiMeRC
National Bioterrorism Civilian Medical Response Center